联想天工iSpirit 3524G/3524F-L3 交换机用户手册

天工网络

责任声明

本手册的目的是帮助用户正确地使用产品，联想网络（深圳）有限公司保留在未预先通知的情况下对本手册内容以及本公司产品进行修改的权利。

本手册不提供任何明示或默示的保证，包括对产品的功能、有关产品的信息以及产品的可销性和对某一特定用途的适用性的默示保证。有关产品保修事宜，请参阅本公司的标准保修服务承诺。对任何因产品或产品操作出现故障而引起的损坏，包括任何利润损失、金钱损失、意外损害或间接损害，以及任何第三方或您为第三方提出的索赔，本公司概不负责。

本手册可能存在编辑上的疏漏，敬请谅解。若有疑问，请与本公司联系。

版权声明

商标所有权

产品序列号：147000966
手册版本： V1.1
出版日期： 2004年2月

目 录

目 录

目 录

目录

目录

目 录

目 录

目 录

本手册指南

读者对象

本用户手册的主要服务对象是负责安装并配置联想天工iSpirit 3524G-L3/3524F-L3交换机的网络或计算机技术人员。在阅读本手册之前用户需要熟悉以太网和交换机的基本概念和术语。

目的

本用户手册主要说明联想天工iSpirit 3524G-L3/3524F-L3交换机的硬件特征和安装、软件配置及常见问题解答。

章节组织

此用户手册包括以下章节：

第 1 章:产品综述，描述交换机的前面板与后面板组成、功能特性、所支持的标准及安装实例。

第 2 章:硬件安装，描述将交换机安装到桌面、机架、机柜及墙上的步骤，并简要说明如何建立交换机的初始配置。

第 3 章:CLI 界面管理，描述 CLI 界面的特征及如何通过 CLI 界面配置交换机。

第 4 章:菜单界面的配置，描述菜单界面的特征及如何通过菜单界面配置交换机。

第 5 章:Web 页面的配置，描述 Web 页面的特征及如何通过 Web 页面配置交换机。

第6章:常见问题解答，描述如何识别并解决交换机安装过程中可能出现的一些问题。

附录 A:产品技术指标，说明交换机的物理和环境指标及相关认证。

附录 B:接口和网线的技术说明，描述接口和网线的技术特征。

本手册规约

本手册假定您熟悉计算机常用词汇，如单击，双击、右键单击、右键双击等，下面的规约将更便于您使用此手册。

注 意 ：该符号表示用户可以记下这部分内容,通常包含对用户有帮助的建议或未包含在本手册中内容的参考。

提 示 ：该符号表示用户需要小心。用户的行为可能导致设备损坏或数据丢失。

警 告 ：该符号表示危险。用户的行为可能导致受伤。用户在设备上工作之前，需要意识到电流带来的危险并熟悉避免意外的标准做法。

文档资料的获取

WWW

你可以在WWW上通过以下站点访问相关文档资料：

http://www.lenovo.com

订购文档

用户可以通过以下网址订购交换机文档CD或其他产品文档：

http://www.lenovo.com

技术支持

通过网站（http://www.lenovo.com）提供在线技术支持。用户可以在该网站获得技术文档、常见问题解答等信息。所购产品处于质保期内的顾客可以通过技术支持中心获得帮助。所有用户都可以通过 Web、E-mail 或邮件等方式反馈意见。用户可以通过在线支持服务解决实际中遇到的技术问题、下载测试软件包、订购学习资料和产品。

技术支持中心为产品处于质保期内的用户提供服务。联系方式如下所示：

E-mail: networks@lenovo.com

Tel: 86755 26955888-6000

文档反馈

如果用户在 WWW 上浏览产品文档，可以通过网页提交技术意见。点击页面上的反馈键,填写页面中的表格,按下提交键,用户就可以将意见提交。

用户也可以将反馈意见以电子邮件形式发送以下邮箱:

networks@lenovo.com

用户还可以将反馈意见以邮件形式邮寄到本公司。用户把反馈意见寄至以下地址:中国广东省深圳市高新技术产业园南区高新南一道联想研发中心大厦,邮政编码:518057。

第 1 章

产品综述

本章主要描述联想天工iSpirit 3524G-L3/3524F-L3**交换机的前面板与后面板的组成、功能特性、所支持的标准及应用举例。本章包括以下内容**:

1、**产品概述**
2、**产品特性**
3、**标准协议**
4、**基本功能概述**
5、**交换机前面板说明**
6、**交换机后面板说明**
7、**应用举例**

1.1 产品概述

联想天工iSpirit3524G-L3/3524F-L3交换机是联想网络推出的面向各种规模的网络接入、汇聚而定制的智能千兆三层以太网交换机。可支持802.1Q VLAN、802.1X完整的生成树协议，端口带宽限制、ACL访问列表控制等特性，并支持RIPv1,RIPv2等动态路由协议，可为各种规模网络提供高性价比的智能多层交换解决方案。

联想天工iSpirit 3524G-L3交换机，支持光纤铜线自动切换，采用200MHz中央处理器，具有32MB SDRAM,提供24个10/100Base-T端口、1个1000Base-X千兆光纤GBIC端口、2个10/100/1000Base-T铜线端口，它的所有接口都支持IP线速路由和无阻塞全线速二层交换。背板带宽为13.6Gbps,包处理能力为6.6Mpps。

联想天工iSpirit 3524F-L3交换机，采用350MHz中央处理器，具有64MB SDRAM,提供24个10/100Base-T端口和2个扩展接口，分别可插1000M光纤模块、10/100/1000Base-T自适应的RJ45端口模块，它的所有接口都支持IP线速路由和无阻塞全线速二层交换。背板带宽为13.6Gbps,包处理能力为6.6Mpps。

联想天工iSpirit 3524G-L3/3524F-L3交换机集本公司的5大Hyper系列技术（超级安全Hyper-Safety、超级管理Hyper-Management、超级冗余 Hyper-Redundancy、超级诊断Hyper-Watch等专利技术)于一身,配合先进嵌入式操作系统Hyper OS,支持基于Console, Telnet的CLI管理和Menu管理以及Web图形管理，可以为用户搭建高速、安全、便捷的高可靠性的信息网络。

联想天工iSpirit 3524G-L3/3524F-L3交换机的外观如图1-1A和1-1B。

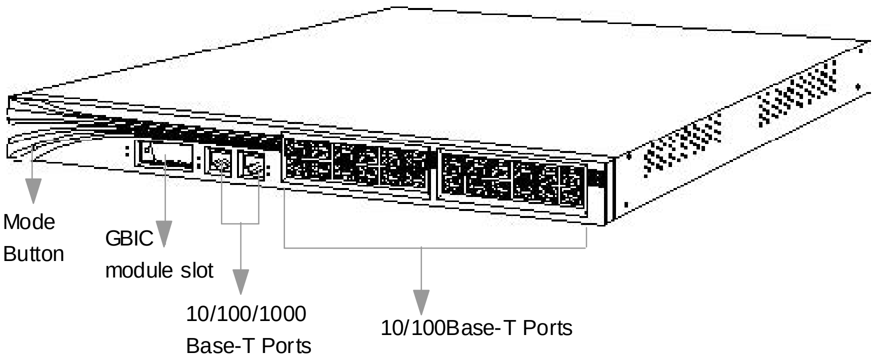


图1-1A 联想天工iSpirit 3524G-L3交换机模型

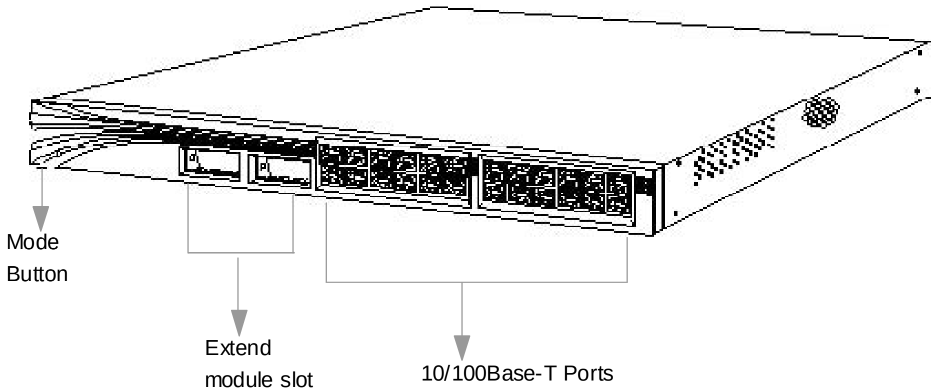


图1-1B 联想天工iSpirit 3524F-L3交换机模型

1.2 产品特性

1.2.1 产品的技术特性

- 10/100 Mbps端口直连网线与交叉网线连接的自协商
- 10/100 Mbps端口自协商和半/全双工操作
- 支持 1000Base-LX、1000Base-SX GBIC 模块（只适用于 3524G-L3 交换机）
- 1000Base-X GBIC光纤接口与10/100/1000Base-T铜线接口的链路冗余热备份、自动检测和自动切换（只适用于 3524G-L3 交换机）
- 支持 100M 单模 / 多模光纤模块、1000M 单模 / 多模光纤模块、10/100/1000Base-T 铜线接口模块（只适用于 3524F-L3 交换机）
- 超距离网线支持能力，最长支持 CAT5 网线距离可达 140 米
- 自动源地址学习
- 8K ARL表
- 提供流量控制，支持 IEEE802.3X 线端阻塞（HOL)和背压（Backpressure)
- 提供4个优先级队列与802.1p的优先级匹配，为多媒体和其它数据流提供灵活的端口优先级机制
- FFP 支持1024 网络数据流，内建基于网络流量的带宽监控和调整
- 网络适配器可以和端口绑定，实现安全访问
- 支持端口聚合，聚合最多可支持 6 组,每组最多支持 8 个速度相同的端口
- 基于端口的 VLAN 和基于 802.1Q tagged VLAN,支持 256 个 VLAN。
- 支持 STP 协议
- 支持 MIBII,RMON（4 种）
- 4种模式LED状态指示灯
- 静态路由功能
- 支持RIPI,RIPII等动态路由协议
- 支持大小为 64 的 IP，MAC 和 PORT 对应的硬件路由表实现快速的三层转发
- 支持 IGMP 侦听
- 支持XModem软件升级
- 支持802.1X认证协议
- 支持嵌入式RADIUS服务器

1.2.2 产品的业务特性

1.2.2.1 强大的三层功能

联想天工iSpirit 3524G-L3/3524F-L3交换机的三层功能包括IP的交换和路由功能。第三层交换的优点在于可以支持第三层的线速路由,而不需要单独的路由器,性能上完全可以取代企业使用的边缘路由器。

1.2.2.2 百兆和千兆聚合技术

联想天工iSpirit 3524G-L3/3524F-L3交换机支持快速以太网以及千兆以太网的链路聚合技术，允许网络管理员将多达8个10/100端口组合到一个通道中，多达6个Trunk group，将2个Gigabit Ethernet组合到一个上行链路通道中。

1.2.2.3 自动备份切换(只适用于3524G-L3交换机）

联想天工iSpirit 3524G-L3交换机特有Hyper-Redundancy技术，25号端口是一个千兆铜线和千兆光纤共用的端口,当千兆铜线口与服务器或其他网络设备相连的时候,如果同时连接光纤接口的时候,交换机会自动切换到千兆光纤口进行工作。当光纤口发生故障的时候又可以自动切换回铜线口,达到实时热备份链路的作用,提高了系统的可靠性和可用性。

1.2.2.4 安全特性

联想天工iSpirit 3524G-L3/3524F-L3交换机支持ARL表的静态设置以及MAC地址与端口的绑定，实现对MAC的控制过滤，独有的Hyper-Safety技术,使得非法主机无法接入网络获取网络资源。

1.2.2.5 强大的网络管理

联想天工iSpirit 3524G-L3/3524F-L3交换机采用Hyper-Management技术，拥有强大和完善的网络管理功能。

◇ 可以利用Console和Telnet口进行Menu或者CLI方式的网络管理配置。
◇ 通过基于SNMP的网管软件可以进行网络管理
◇ 可以基于web的页面管理图形用户接口采用java程序技术编写，操作简单，功能强大，界面直观
◇ 内置多种SNMP的网管代理，Bridge MIB、MIB II、 Entity MIB version 2、RMON MIB和Proprietary MIB
◇ 4组RMON的（1、2、3、9）网管协议（统计量信息、历史信息、告警信息、事件信息）
◇ 易于软件升级设计，可以通过TFTP的带内（in-band）升级方法实现。

1.2.2.6 VLAN

联想天工iSpirit 3524G-L3/3524F-L3**交换机实现的**VLAN**技术支持基于端口的**VLAN**符合通用标准** 802.1Q。

1.3 标准协议

联想天工iSpirit 3524G-L3/3524F-L3**交换机支持的标准和协议见表**1-1

表1-1

协议	参考文档
桥（生成树）	IEEE802.1d
以太网	IEEE802.3
快速以太网	IEEE802.3u
全双工流控	IEEE802.3x
千兆以太网	IEEE802.3z
Link Aggregation	IEEE802.3ad
VLAN	IEEE802.1Q
UDP	RFC 768,RFC 950,RFC 1071
TCP	RFC 793
TFTP	RFC 783
BOOTP	RFC 906,RFC 951,RFC 1350
IP	RFC 791
ICMP	RFC 792
ARP	RFC 826
Telnet	RFC 854~RFC 859
SMI	RFC 1155
SNMP	RFC 1157
MIB II	RFC 1213 & RFC 1573
Ether-like MIB	RFC 1398
Bridge MIB	RFC 1493
Ether-like MIB	RFC 1643
RMON	RFC 1757
IGMPv2	RFC 1112
DHCP	RFC 2131
RIPv1,RIPv2	RFC1058,RFC1724

1.4 基本功能概述

1.4.1 端口聚合（Port Trunking）

Port Trunking技术是一种将网络流量聚集在一组端口上的方法,以形成一个交换机之间的大容量的通道或容错的通道,通道之间可以实现流量均衡。联想天工iSpirit 3524G-L3/3524F-L3 交换机支持 Port Trunking，通过创建 Port Trunking 来提升交换机之间的带宽。Port Trunking把多个物理端口捆绑在一起当作一个逻辑端口来使用。

1) 如果 Port Trunking 中的一个端口发生堵塞或故障，那么数据包会被重新分配到该 Port Trunking 中的别的端口进行传输。
2)如果这个故障端口重新恢复正常,那么数据包将重新分配到该Port Trunking中的所有端口进行传输。
3) 联想天工iSpirit 3524G-L3/3524F-L3交换机的Port Trunking功能与Intel和Cisco的同类产品的 Port Trunking 功能兼容。

1.4.2 虚拟局域网（VLAN）

1.4.2.1 VLAN概述

VLAN主要是指看起来好象在同一个物理局域网中通信的设备集合。任何一个端口的集合（甚至交换机上的所有端口）都可以被看作是一个 VLAN。VLAN 的划分不受硬件设备物理连接的限制，用户可以通过命令灵活地划分端口创建定义 VLAN。

VLAN 功能使您在构建自己的广播域时，不再受限于网络的物理连接。一个 VLAN 就是一群独立于具体网络拓朴的局域网设备，它们在通讯时，不论如何连接，属于VLAN的所有设备都好像在一个真正的物理局域网上。

VLAN 的具体作用体现在：

1)可以控制广播数据，流量限制其广播的范围。假设在 VLAN“研发部”中的一个设备发出了一个广播报文，那么只有‘研发部’这个VLAN中的设备才能收到该广播报文。其他部门将不会收到该广播报文。
2)提供了额外的安全特性。跨 VLAN 的访问只有通过三层转发，不能直接访问。
3)简化了设备在网络中的移动和管理。

具体地讲，VLAN 技术是为了创建第三层逻辑广播域，VLAN 可在一个交换机上划分，也可以跨越多个交换机划分。VLAN 实现了在物理上是一个网段的交换机群之间进行逻辑 VLAN 划分，即分成多个逻辑广播域，避免广播风暴的发生。

1.4.2.2 VLAN的分类

iSpirit 3524G/F-L3支持基于端口Vlan的划分。这种划分是把一个或多个交换机上的几个端口划分一个逻辑组，这是最简单、最有效的划分方法。该方法只需网络管理员对网络设备的交换端口指定VLAN即可，不用考虑该端口所连接的设备。IEEE802.1Q规定了依据以太网交换机的端口来划分VLAN的国际标准。使不同厂商的设备可以同时在一个网络中使用，各自的VLAN设置可以被其他设备所识别，实现互通。根据IEEE802.1Q，端口可以标志Tagged和Untagged，Tagged/Untagged标志该端口所连接的设备是否能够支持带有802.1Q Tag header的帧。3524G/F-L3交换机一个端口可以属于多个Tagged VLAN ID和多个Untagged VLAN ID。VLAN ID的范围为1到4094，交换机最多支持256个VLAN。

1.4.2.3 Tagged VLAN的应用

标签（Tagging）最常应用在跨交换机VLAN中。此时，交换机之间的连接通常叫做中继。使用标签后，可以通过一个或多个中继创建多个交换机的VLAN。一个VLAN可以很轻易地通过中继跨多个交换机。

使用Tagged VLAN的另一个好处就是一个端口可以属于多个VLAN。这一点在当您有一个设备（例如服务器）必须属于多个VLAN的时候特别有用。这个设备必须有支持802.1Q的网络接口卡。

1.4.2.4 指定VLAN标签

每个VLAN都可以赋予一个802.1Q VLAN Tag。当端口被加到一个802.1Q标签定义好的VLAN中去时，您可以决定该端口是否使用该VLAN的标签。交换机的缺省模式是所有端口都属于一个叫default的VLAN中，但不使用该VLAN的标签（VLANid）

并不是所有端口都可以使用标签。当数据流从交换机的一个端口输出时，交换机实时决定是否需将该VLAN的标签加到数据包中。交换机根据VLAN的端口的配置情况决定加上或者去掉数据包中的标签。

1.4.2.5 混合使用Tagged VLAN和Port-Based VLAN

您可以混合使用Tagged VLAN和Port-Based VLAN。一个给定的端口可以属于多个VLAN，前提是该端口只能在一个VLAN中是未加标签的（Untagged）。换句话说，一个端口同时能属于一个Port-Based VLAN和多个Tagged VLAN。

1.4.3 STP（Spanning Tree Protocol）

联想天工iSpirit 3524G-L3/3524F-L3交换机支持IEEE802.1d标准的STP协议，STP是运行在Bridges和Switches层上并与802.1d协议标准兼容的第二层协议。这一协议提供了网络的动态冗余切换机制。因此，使用STP，可以让您在网络设计中部署备份线路，并且保证：

1)在主线路正常工作时，备份线路是关闭的。

2)当主线路出现故障时，自动激活备份线路，将数据流切换到备份线路，保证设备正常运行。

由此可见，使用STP，可以保证当在网络结构上存在冗余路径情况下，阻止网络回路发生。网络回路对网络来说是致命的打击，冗余链路作为网络备份路径又是非常重要的 。

1.4.4 ARL 表

ARL是Address Resolution Login的简称，是二层交换机硬件转发数据帧的核心。联想天工iSpirit 3524G-L3/3524F-L3交换机分开存储单播和多播mac地址分别为arl和marl。硬件根据数据帧的目的MAC地址查arl和marl表找到相应的表项，并把数据帧送到表项指定的输出端口。表项可以通过交换机输入端口发数据被交换机自动学习生成的，也可以管理员向arl和marl中添加。

1.4.5 路由

在一个划分为不同子网的网络中，如果一个子网接收到的数据包上的目的IP地址包含的网络号与本子网的网络号不同的话，此时，就需要路由设备来决定这些数据包的流向。也就是说，这些数据包首先发送到路由设备，然后再向目的主机转发。

联想天工iSpirit 3524G-L3/3524F-L3交换机支持静态路由和动态路由，用户可在路由配置模式下配置交换机的静态路由信息。静态路由是由用户定义的、一条可使数据包从源地址通过指定路径到达目的地址的路由。当动态路由协议未能创建一条到特定目的的路由时，静态路由就显得特别重要。还可以通过配置某一静态路由为默认路由，把无路由的数据包发送到默认的网关。动态路由通过路由协议来创建路由项，联想天工iSpirit 3524G-L3/3524F-L3交换机支持RIPI,RIPII路由协议。

1.4.6 RIP

RIP是Routing Information Protocol的简称，RIP（路由信息协议）是一个内部网关协议（IGP），主要应用在中等规模的网络，RIP协议采用距离向量算法，在路由信息中包括了到达IP目的（向量）的跳跃次数（距离），跳跃次数最小的路径是最优路径。RIP允许的最大跳跃次数为15，需要跳跃16次及其以上的目的地址被认为是不可达的。

RIP路由器通过周期性广播(缺省为30秒)来与邻近的RIP路由器交换路由信息，广播的时间间隔可以设定。广播的内容就是整个路由表。

当RIP路由器收到邻近路由器的路由表后，要经过计算来决定是否更新自己的路由表。如果自己的路由表需要更新，路由器在更新完毕后会立即把更新的内容发送到邻近的路由器而不必等待广播间隔时间的结束。有如下原因会引起路由表的变化：

- 启动了一个新的接口
- 使用中的接口出现了故障
- 邻近路由器的路由表改变
- 路由表中的某条记录的生存周期结束，被自动删除

RIP路由器要求在每个广播周期内，都能收到邻近路由器的路由信息，如果收不到，路由器将会经过如下过程后放弃这条路由：

- 如果在90秒内没有收到，而且它邻近具有相同跳跃次数（HOP）的路由存在，现有路由将被取代;
- 如果在180秒内没有收到，该邻近的路由器被认为不可达。

1.5 交换机前面板说明

3524G-L3**交换机前面板包含**24**个**10/100Base-T RJ-45**端口、**1**个**1000Base-X GBIC**模块插槽、**2 **个** 10/100/1000Base-T **端口、端口** LED **状态指示灯、模式** LED **状态指示灯和模式键等组件（如图** 1-2A **所示）。**

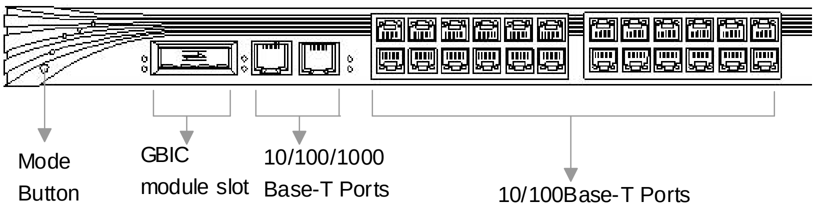


图**1-2A 3524G-L3**交换机前面板

3524F-L3**交换机前面板包含**24**个**10/100Base-T RJ-45**端口、**2**个模块扩展插槽、端口**LED **状态指示灯、模式**LED **状态指示灯和模式键等组件（如图**1-2B **所示）。**

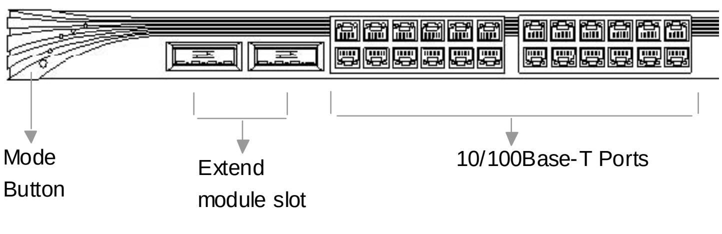


图**1-2B 3524F-L3**交换机前面板

1.5.1 10/100Base-T 端口

交换机 10/100Base-T 端口（如图 1-2A 和 1-2B 所示）可以连接的网络设备的最远距离是 140 米。其可连接的网络设备包括：

- ➲10Base-T 兼容设备，如通过 RJ-45 接口和 CAT3、CAT4、CAT5 或 CAT5E 网线连接的工作站或集线器。
- ➲100Base-TX 兼容设备，如通过 RJ-45 接口和 CAT5 或 CAT5E 网线连接的高速工作站、服务器、路由器、集线器或其他交换机。

注 意 ：

❶ CAT3、CAT4 网线只可以承载 10Mbps 数据流，而 CAT5、CAT5E 网线可以承载 100Mbps 数据流。

❷ 10/100Base-T端口网线直连与交叉连接自协商。

可以以任意组合将交换机 10/100Base-T 端口设置成半双工、全双工、十兆或百兆端口。也可以遵循IEEE802.3u将端口设置成速度和双工的自协商。当端口设置了自协商后，端口会自动感知与其连接设备的速度和双工设置并通知该设备端口的性能。如果与其连接的设备也支持自协商，则交换机端口会将连接调整到最好状态（即速度设置为双方都支持的最快的速度，如果与交换机相连的设备支持全双工则双工设置为全双工），同时把自己的状态作相应调整。

注 意 ：

根据 IEEE802.3u 的标准，自协商过程需要建立双方交互协商的连接，我们推荐用户将交换机端口以及与其连接的设备端口设置为自协商，这样可以保证交换机的自适应功能将连接调整到最佳状态。

1.5.2 GBIC 模块插槽(只适用于 3524G-L3 交换机)

3524G-L3交换机带有一个GBIC插槽，装入一个GBIC模块可以与光纤相连。目前支持的GBIC模块类型及每种类型支持最长光纤如表1-2所示。

表1-2

模块类型	介质	波长	最长支持长度
1000Base-SX	62.5um多模光纤	850nm	275m
	50um多模光纤		550m
1000Base-LX	62.5um多模光纤	1310nm	550m
	50um多模光纤		550m
	10um单模光纤		5000m
1000Base-ZX		1550nm	100000m

图1-3说明如何将一个GBIC模块(可选)插入交换机GBIC模块插槽。

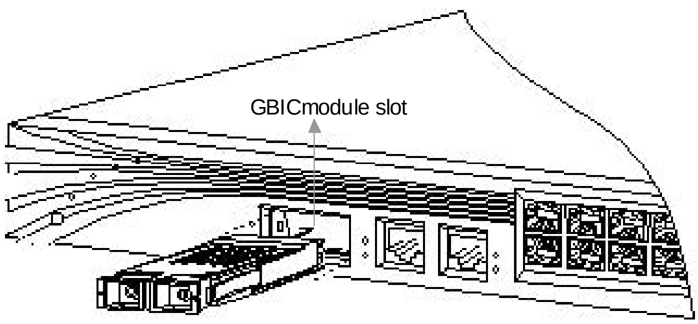


图1-3 将一个GBIC 模块插入交换机GBIC 插槽

1.5.3 扩展模块插槽(只适用于 3524F-L3 交换机)

iSpirit 3524F-L3交换机有两个扩展模块插槽，可插100M单模/多模光纤模块、1000M单模/多模光纤模块、10/100/1000Base-T铜线端口，10/100/1000Base-T铜线端口见1.5.4 节所述。各端口支持的光纤参数如表 1-3 所示：

表1-3

光纤模块类型	介质	波长	最长支持长度
100M单模	62.5um多模光纤	1300nm	20000m
	50um多模光纤		
100M多模	62.5um多模光纤	1300nm	2000m
	50um多模光纤		
1000M单模	62.5um多模光纤	1300nm	550m
	50um多模光纤		550m
	10um单模光纤		10000m
1000M多模	62.5um多模光纤	850nm	220m
	50um多模光纤		500m

如图 1-4 所示，将模块插入 iSpirit 3524F-L3 交换机的步骤如下：

- ➲将模块沿导轨插进扩展模块插槽
- ➲确保模块与插槽完全接触
- ➲ 上紧螺丝

将模块从iSpirit 3524F-L3交换机的插槽上拔下来的步骤如下:

- ➲ 拧松模块档板左右两边螺丝，使其脱离机箱面板
- ➲ 两手捏紧模块档板左右两边螺丝，平衡往外抽拉，使模块脱离机箱

注意：扩展模块不支持热插拔，在插拔前必须将交换机断电。否则可能损坏交换机。

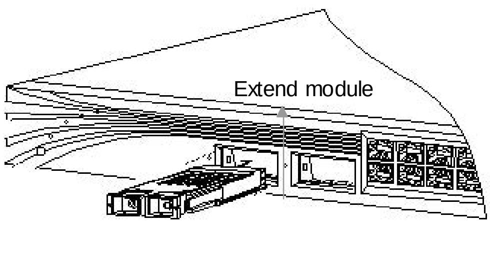


图1-4 将模块插入交换机扩展模块插槽

1.5.4 10/100/1000Base-T 端口

交换机10/100/1000Base-T端口可以连接的网络设备的最远距离是140米。其可连接的网络设备包括：

➲10Base-T 兼容设备，如通过 RJ-45 接口和 CAT3、CAT4、CAT5 或 CAT5E 网线连接的工作站或集线器。

➲100Base-TX 兼容设备，如通过 RJ-45 接口和 CAT5 或 CAT5E 网线连接的高速工作站、服务器、路由器、集线器或其他交换机。

➲1000Base-T 兼容设备，如通过 RJ-45 接口和 CAT5 或 CAT5E 网线连接的千兆工作站、服务器、路由器或其他交换机。

注 意 ：

❶CAT3、CAT4 网线只可以承载 10Mbps 数据流，而只有 CAT5、CAT5E 网线可以承载 100Mbps 和 1000Mbps 数据流。

❷10/100/1000Base-T端口如果工作在10/100Base-TMbps数据传输速率下网线直连与交叉连接自协商,而如果该端口工作在1000Mbps数据传输速率下网线不支持直连与交叉连接的自协商。

该端口在 10/100Mbps 数据传输率时可以以任意组合将端口设置成半双工、全双工、十兆或百兆端口。在 1000Mbps 数据传输率时该端口设置为半双工 / 全双工模式。

该端口的缺省设置是自协商，遵循 IEEE802.3ab 标准。

注 意 ：

iSpirit 3524F-L3 交换机的25 口可以强制成100Mbps 全双工、半双工，1000Mbps 全双工、半双工或自适应模式（缺省），26 口只能在自适应模式（缺省）。

1.5.5 LED 状态指示灯

用户可以通过LED灯监测交换机的活动和性能。每个端口或GBIC模块插槽都有一对link状态指示灯和模式指示灯，link-LED、mode-LED和模式键位置如图1-5A和1-5B所示。

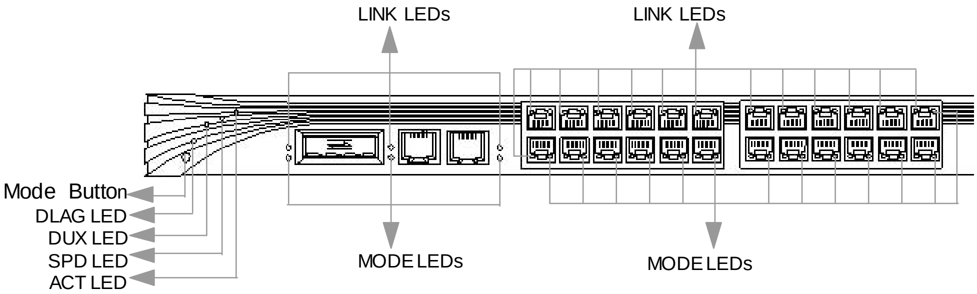


图1-5A 3524G-L3 LED 状态指示灯、模式键和端口LED状态指示灯位置图

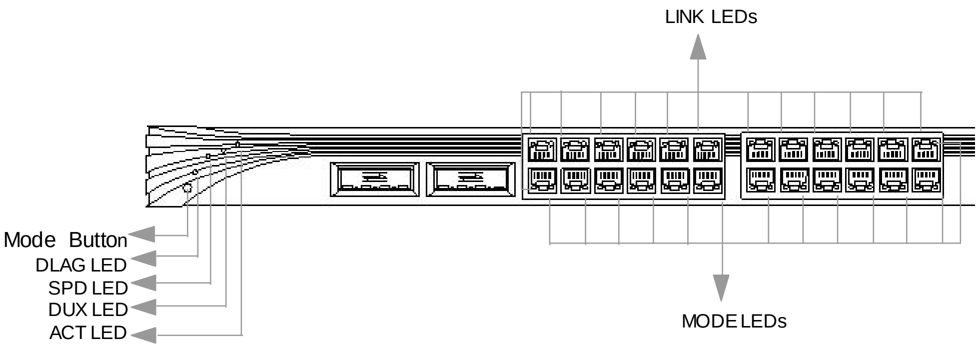


图1-5B 3524F-L3交换机LED 状态指示灯、模式键和端口LED状态指示灯位置图

1.5.5.1 模式指示灯和模式选择

用户按模式键可以使端口模式指示灯显示相关模式信息。用户可以选择 ACT、SPD、DUPX 和 DIAG 四种模式。各模式的含义如表 1-4 所示。

表 1-4：

模式LED指示灯	端口模式	说明
ACT	端口收发数据状态	说明端口收发数据状态，是缺省模式
SPD	端口速度	端口运行速度：10、100、1000Mbps
DUPX	端口双工	端口双工模式：全双工或半双工
DIAG	端口诊断	诊断端口是否有故障

1.5.5.2 端口LED状态指示灯

表1-5说明端口状态指示灯的颜色及相应含义。表1-6说明不同模式下端口LED模式状态指示灯的颜色及相应含义。

表 1-5：端口 LED 连接状态指示灯颜色的含义

端口	颜色	状态
连接端口	无	无连接
	绿	连接

注 意 ：

3524G-L3交换机的1000Base-XGBIC模块和靠近该端口的10/100/1000Base-T端口都正常连接网线的情况下，只有一个端口正常工作。所以只有一个端口的连接LED指示灯和模式LED指示灯正常显示端口的信息。1000 Base-X端口的优先级更高，即GBIC模块连接到GBIC插槽后，GBIC插槽对应的LED灯正常显示第25端口的信息。

表 1-6：端口 LED 模式状态指示灯颜色的含义

端口模式	端口LED状态指示灯颜色	端口状态
ACT	无	无数据
	闪烁绿色	端口在发送或接收数据
SPD	10/100Base-T端口	
	无	端口以10Mbps运行
	绿色	端口以100Mbps运行
	1000Base-X GBIC模块	
	绿色	端口以1000Mbps运行
	10/100/1000Base-T端口	
	无	端口以10Mbps或100Mbps运行
	绿色	端口以1000Mbps运行
DUPX	10/100Base-T端口	
	无	端口在半双工模式下工作
	绿色	端口在全双工模式下工作
	1000Base-X GBIC 模块	
	绿色	端口在全双工模式下工作
	10/100/1000Base-T端口	
	无	端口在半双工模式下工作
	绿色	端口在全双工模式下工作
DIAG	无	端口正常工作
	闪烁绿色	端口故障

1.6 交换机后面板说明

交换机后面板包括一个 AC **电源接口和一个** UART **控制端口（如图** 1-6A,1-6B **所示）。**

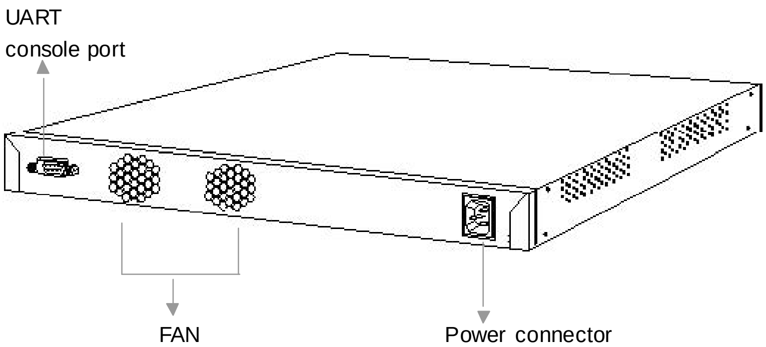


图1-6A 3524G-L3交换机后面板

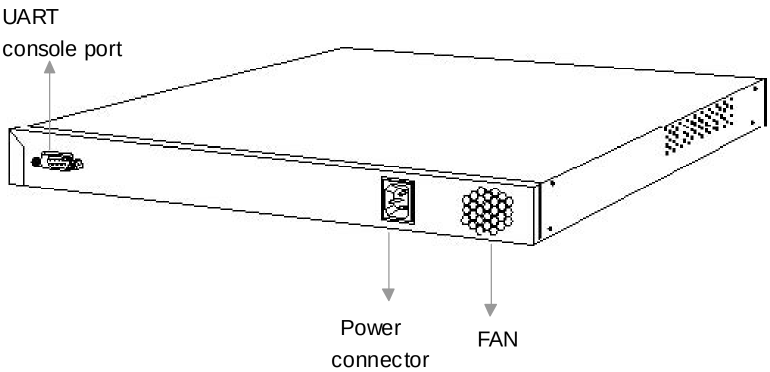


图1-6B 3524F-L3交换机后面板

1.6.1 电源接口

交换机支持从180伏到240伏的交流电压。使用时需要用交流电缆将电源接口与电源插座连接起来。

1.6.2 串口

用户可以通过使用UART串口和随机提供的专用控制端口电缆将交换机与一台PC机相连以实现对交换机的管理。控制端口电缆接插件的管脚配置参见附录B。

1.7 应用举例

本节我们将通过实例说明怎样使用交换机创建专用的计算机网络,如何利用快速以太网和千兆以太网将不同的网络整合起来。

1.7.1 设计思路

随着网络用户的不断增多,带宽成为制约网络数据传输的瓶颈。当设计者配置网络的时候，需要考虑: 1）网络用户需要的带宽；2）网络用户使用的网络应用优先级。下文说明造成网络性能下降的原因及如何配置网络以增加给用户提供的带宽。

网络需求 1

在一个网段上的用户很多，这其中有越来越多的用户访问Internet.

建议设计方案 1

创建较小的网络分段，以使较少的网络用户分享带宽。

把网络资源与经常使用这些资源的用户放在一个逻辑网段上。

在交换机和与其相连的工作站之间建立全双工工作模式

网络需求 2

新型 PC 机、工作站、服务器的功能越来越强大

网络应用（如带大附件的 email 或多媒体）对网络带宽的高需求

建议设计方案 2

将网络用户需要平等访问的服务器或路由器直接与交换机的快速以太网口或千兆以太网口相连以使他们拥有自己的快速以太网段或千兆以太网段.

1.7.2 应用举例

在交换式局域网络，最常见的拓扑是层次结构。一般分为三层：用户所在的接入层，服务器与路由器所在的分布层以及连接办公室或者建筑物链路的核心层或者骨干层。联想天工 iSpirit 3524G-L3 交换机适用于分布层（即汇聚层）、接入层和小型网络核心层的应用，它能为与直接连接桌面的工作组交换机相连，还能提供到核心层或骨干层的高速接入（千兆上连），提供千兆以太网模块可适用于上连高速率主干网络，用以有效的缓解网络主干的瓶颈。由于具有三层交换功能，还可以在一些中小型企业网络中用来做中心交换，这样可以利用较少的投资来实现企业级的网络应用，性能价格比非常高。

典型应用如图，联想天工 iSpirit 3524G-L3 交换机位于汇聚层，向下可以连接多个工作组级交换机，向上连接骨干交换机或者全千兆交换机，为用户接入提供骨干为 1Gbps 的速率，同时完成路由功能和快速的 IP 交换。

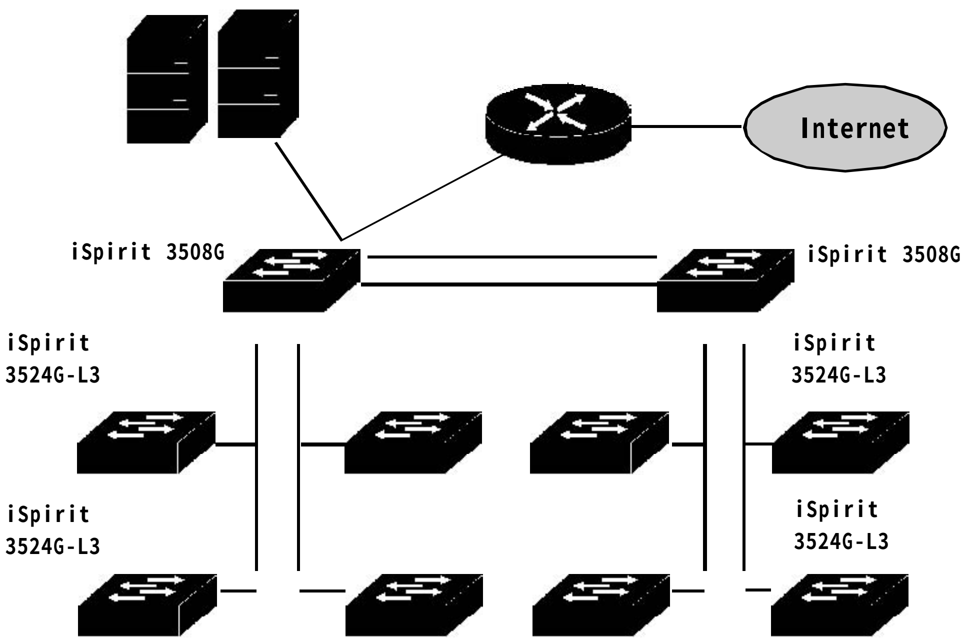


图1-7 联想天工iSpirit 3524G-L3交换机位于汇聚层应用

第2章

交换机的安装与启动

本章主要说明如何正确安装并启动联想天工iSpirit 3524G-L3/3524F-L3**交换机及如何上电自检测**(POST)**以确保交换机正常操作。用户需要仔细阅读以下内容并按顺序进行操作。**

1、**安装前指南**
2、**安装步骤**
3、**上电过程**
4、Bootrom **启动选项介绍**
5、**连接步骤**

2.1 准备安装

在安装之前,用户需要仔细阅读以下警告内容,对于任何因安装使用不当而造成的直接、间接、有意、无意的损坏及隐患，本公司概不负责。

警告 :只允许经过培训有资格的技术人员安装或替换该设备。
警告 :在将设备与电源连接之前用户需要仔细阅读本用户手册。
警告 :在带电设备上工作之前，用户需要摘掉金属饰品（包括戒指、项链、手表等)。金属物品与电源和大地相连时会迅速升温，可能导致严重烧伤或将金属物品熔化在终端上。
警告 :不要将机箱放在其他设备上。如果机箱坠落可能造成严重的身体伤害或设备损害。
警告 :用户需要确保随时可以方便的关闭插座将设备断电。
警告 :为防止交换机温度过高，不要在超过建议的 45°C（113 °F）环境温度下
警告 :运行机器。为避免通风限制，在通风口前 7.6cm（3 英寸）处不放置杂物 。
警告 :该设备在 TN 电源系统下正常工作。
警告 :当安装设备时，地线必须最先连接、最后断开。
警告 :该设备依赖建筑物的相应短路保护措施。注意在相导体上安装了保险丝或断路开关。
警告 :该设备需要接地。注意通常使用过程中要将主机接地。
警告 :将设备与电源相连时需要小心，防止线路超负荷。
警告 :电压不匹配可能造成设备损坏或火灾。如果设备标签上所示的电压与电源插座上的电压不相符，不要将设备与其相连。
警告 :交换机上如果没有开关，启动前需要断开电源线。
警告 :电源线未断开前不要接触电源。对于一个有电源开关的系统，当电源开关已关闭而电源线未断开时，电源内的线电压仍然存在。而对于一个没有电源开关的系统，在电源线未断开时，电源内的线电压也仍存在。
警告 :户外有闪电时不要在系统上工作或连接、断开网线。
警告 :该产品的最终处理符合国家的法律法规。

2.1.1 安装指南

交换机可以安装在桌面、机架、机柜或墙上。在安装之前首先需通过给交换机上电并运行POST以确认交换机工作正常。其步骤参见“上电过程”。

警 告 ：

交换机里没有可用部件。如果用户拧开螺丝、打开机箱或拆开交换机都将使保修单无效。

2.1.1.1 安装位置指南

用户决定在何处安装该交换机时，请参照以下指南：

❶ 从交换机10/100Base-T和10/100/1000Base-T端口到所连设备的最长距离不超过100米。

❷ 从交换机1000Base-X端口到所连设备的最长距离不超过10,000米。

❸ 布线需要远离电磁干扰，如收音机、电源线或荧光灯。

❹ 交换机前后面板空间具体说明如下：

.可以清晰看到前面板指示灯

.可以方便地访问端口以使布线不受限制

.电源线可以将后面板电源接口与AC电源插座相连

.后面板通风孔附近3英寸空间内无杂物阻挡风流

❺ 附录A中说明交换机的运行环境。

❻ 交换机周围与通风口处的空气流通不受限制。

❼ 交换机周围的温度不超过40^{0}C

注意：

如果交换机安装在一个封闭的多层的机柜中其周围的温度会比正常温度高。

2.2 安装步骤

下面以3524G-L3交换机为例说明交换机的安装步骤。

2.2.1 在桌面或机架上安装交换机

在桌面或机架上安装交换机时，请参考以下步骤：

❶ 从安装包中拿出四个带胶条的橡胶垫。去掉橡胶垫上胶贴，将四个橡胶垫粘到交换机底部凹陷处。

❷ 将交换机放到靠近 AC 电源的桌面或机架上。

❸ 使用电源线将交换机与电源插座相连。连上电源以后，系统首先开始POST检测，这部分内容参考“ 上电过程 ”。

2.2.2 在机柜里安装交换机

警 告 ：

为避免安装或使用机柜中交换机时造成身体伤害,用户必须采取有效的预防措施以确保交换机的稳固。请参阅以下指南以保证安全:

➲ 如果机柜内只有一台交换机，请把它安装到机柜底部。

➲ 如果机柜内有若干组件，请将其中组件按轻重顺序由上至下摆放。

➲ 如果机柜有固定装置，请先安装固定装置再安装交换机。

随交换机提供的机柜安装法兰可以安装在一个19英寸或24英寸的机柜上，其上安装孔参见图 2-1。

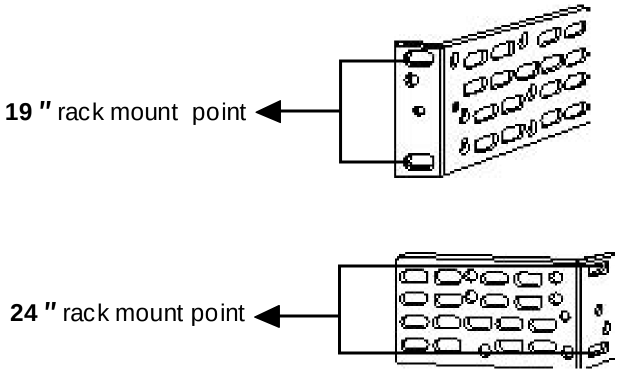


图2-1法兰安装孔

为了将交换机安装到一个19**英寸或**24**英寸标准机柜中，需要参照以下步骤：**

- ❶ **从交换机上拧下螺丝**
- ❷ **将法兰安装在交换机上**
- ❸ **将交换机安装到机柜里**

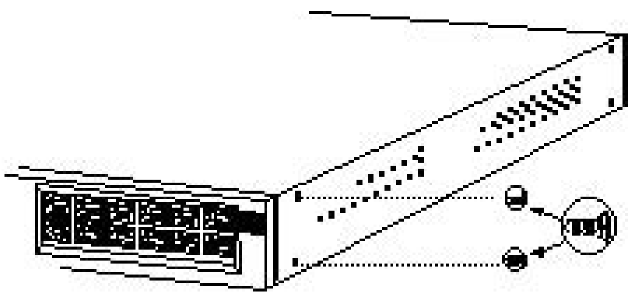


图2-2 从交换机上拧下螺丝

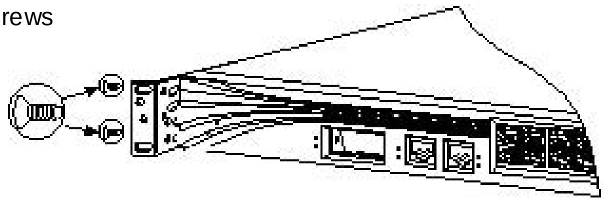
2.2.2.1 将法兰安装在交换机上

法兰的方向及使用螺丝的选择需要根据用户选择的19**英寸或**24**英寸的机柜而定。根据以下指南分别在每个法兰上安放两个螺丝。**

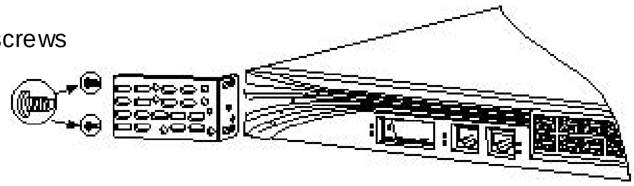
对于 19 **英寸机柜，用随机提供的螺丝将法兰的长边安装在交换机上。**

对于 24 **英寸机柜，用随机提供的螺丝将法兰的短边安装在交换机上。**

图 2-3、**图** 2-4 **分别显示如何将法兰安装在交换机的前部和后部。在相反方向进行同样的安装。**

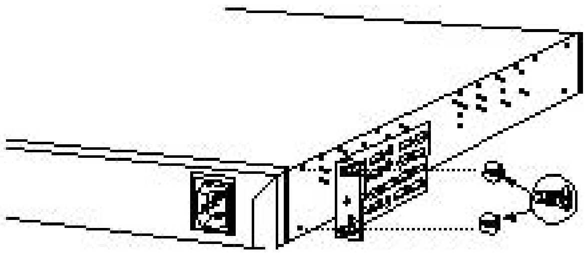


19″Configuration



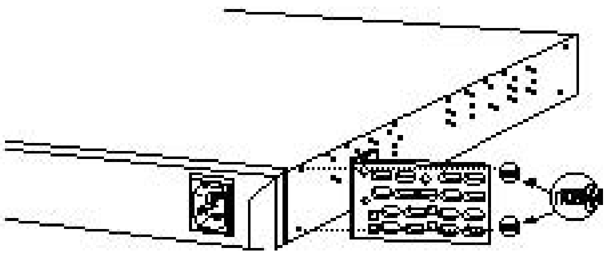
24″Configuration

图2-3将法兰安装在交换机前部



flat-head screws

19″ Configuration



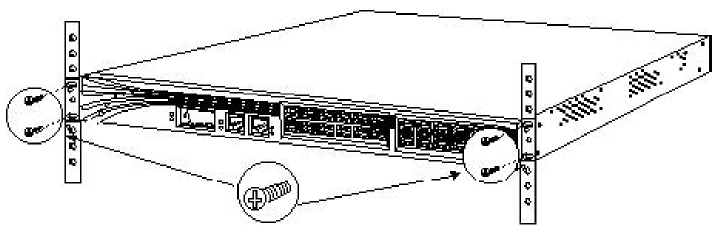
flat-head screws

24″ Configuration

图2-4将法兰安装在交换机后部

2.2.2.2 将交换机安装到机柜里

把法兰安装在交换机上后，使用4**个随机提供的螺丝将法兰安全固定在机柜里（如图**2-5**所示），然后把电源线插到交换机上。连上电源以后，系统首先开始**POST**检测。这部分内容参考“上电过程”。**



machine screws

图2-5将交换机安装到机柜里

2.2.3 在墙上安装交换机

为了把交换机安装到墙上，需要进行以下步骤：

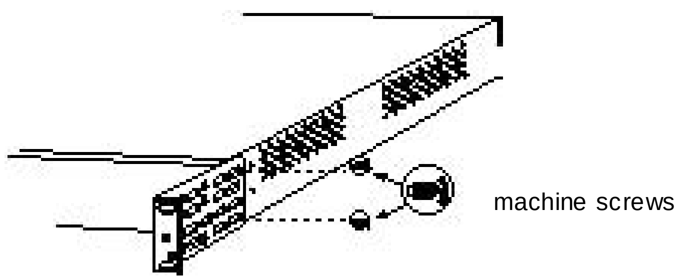
❶将法兰安装到交换机上

❷将交换机安装到墙上

2.2.3.1 将法兰安装到交换机上

根据需要用户可以选择将交换机水平或垂直安装在墙上。

水平/垂直安装交换机：使用随机提供的螺丝将法兰的长边装在交换机上,将法兰的长边装在墙上,如图 2-6 **所示。**

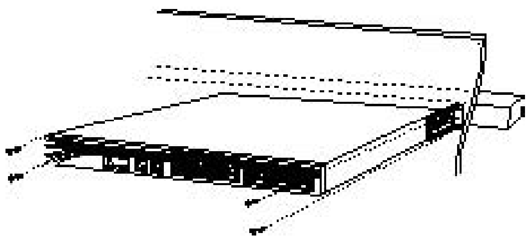


For wall-mounting

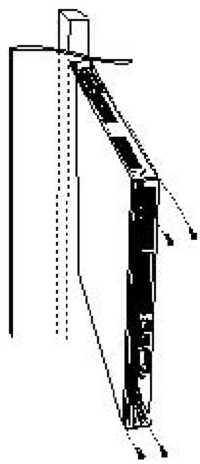
图2-6将法兰长边安装到交换机

2.2.3.2 将交换机安装到墙上

为了最好地支撑交换机及网线，用户需要确定将交换机安装在壁柱或安装板上（如图2-7 所示），然后把电源线插到交换机上。



水平安装到墙上



垂直安装到墙上

图2-7将交换机安装到墙上

2.3 上电过程

2.3.1 运行 POST 检测

安装好交换机后打开交换机需要进行以下步骤：

❶ 电源线与交换机上的 AC 电源接口相连；

❷ 电源线的另一端与 AC 电源插座相连。

交换机上电后前面板 26 个端口指示灯全部亮起，随后熄灭，按上电自检的进程，前面板端口指示灯再逐个亮起。当前面板端口指示灯全部亮起，表示交换机已经经过POST 检测，端口指示灯进入正常工作状态，在 ACT 模式下指示灯正常显示，表示交换机工作正 常 。

如果你的交换机不能通过 POST 检测，请立即通知交换机授权供应商。

2.4 连接步骤

以3524G-L3交换机为例说明如何连接交换机。

2.4.1 连接交换机 10/100 Mbps 端口

交换机10/100 Mbps端口配置成以所连设备的速度运行。如果所连设备不支持自动协商，用户可以手工设定速度或双工模式等参数。根据以下步骤将交换机与 10Base-T 或 100Base-TX 设备相连：

➲ 对于 10Base-T 设备使用 CAT3、CAT4、CAT5 或 CAT5E 直连或交叉网线与交换机前面板的RJ-45端口相连。对于100Base-TX设备使用CAT5或CAT5E直连或交叉网线与交换机前面板的 RJ-45 端口相连（如图 2-8 所示）。网线的管脚说明参见附录 B。

➲ 将网线的另一端与所连设备的 RJ-45 端口相连。当交换机与所连设备建立连接之后，相应端口 LED 连接状态指示灯会亮。如果该灯不亮，可能是连接设备没开机，连接线路有问题或连接设备的网卡有问题。参考第 5 章解决相关问题。

➲ 如果需要的话，重新配置并重启设备。

➲ 重复 1 至 3 步以将每一个设备连接到 10/100 Mpbs 端口。

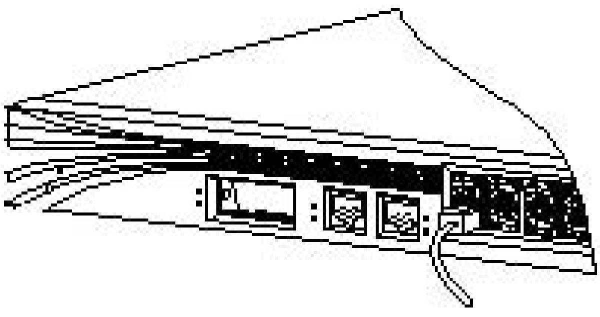


图2-8连接交换机10/100Base-T端口

2.4.2 连接交换机 1000Base-X GBIC 模块端口（只适用于 3524G-L3 交换机）

根据第一章描述内容将GBIC模块插入GBIC模块插槽。

提 示 ：

用户在没有准备好连接光纤前,请不要拔掉光纤端口的橡胶塞和光纤上的橡胶盖,以免光纤端口和光纤受到污染物或周围光线的损坏。

用户进行以下操作与1000Base-X端口相连：

❶ 从 GBIC 模块的光纤端口拔下橡胶塞，把橡胶塞妥善保管好以备后用。

❷ 将 SC 接口插入光纤端口，如图 2-9 所示。

❸将网线的另一端与所连设备的1000Base-X端口相连。当交换机与所连设备建立连接之后，相应端口 LED 连接状态指示灯会亮。如果该灯不亮，可能是连接设备没开机，连接线路有问题或连接设备的网卡有问题。参考第 6 章解决相关问题。

❹ 如果需要的话，重新配置并重启设备。

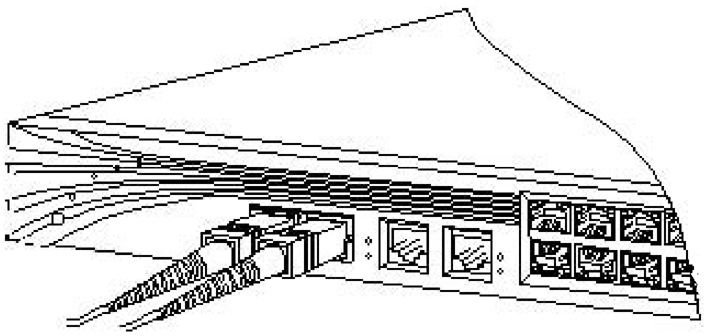


图2-9连接交换机1000Base-X端口

2.4.3 连接交换机 100Base-X光纤模块端口或 1000Base-X光纤模块端口(只适用于 3524F-L3 交换机)

根据第一章描述内容将100Base-X 光纤模块和1000Base-X 光纤模块插入扩展模块插槽（不可热插拔）。

提示：
用户在没有准备好连接光纤前，请不要拔掉光纤端口的橡胶塞和光纤上的橡胶盖，以免光纤端口和光纤受到污染物或周围光线的损坏。

用户进行以下操作与100Base-X端口或1000Base-X端口相连：

❶从100M光纤模块的光纤端口或1000M光纤模块的光纤端口拔下橡胶塞，把橡胶塞妥善保管好以备后用。

❷将 SC 接口插入光纤端口，如图 2-10 所示。

❸将网线的另一端与所连设备的100Base-X端口或1000Base-X端口相连。当交换机与所连设备建立连接之后，相应端口LED连接状态指示灯会亮。如果该灯不亮，将光纤和交换机重新连接，如果还是没亮则可能是连接设备没开机，连接线路有问题或连接设备的网卡有问题。

❹如果需要的话，重新配置并重启设备。

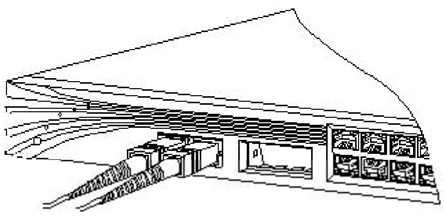


图2-10　将SC接口插入光纤端口

2.4.4 连接交换机 10/100/1000Base-T 端口

交换机10/100/1000Base-T端口配置成以所附设备的速度运行。如果所附设备不支持自动协商，用户可以手工设定速度和双工模式等参数。

注 意：

交换机10/100/1000Base-T端口连接1000Base-T设备时,端口和所连设备的双工模式必须是全双工。

如果该端口与 10Base-T 或 100Base-TX 设备相连，相应操作与第 2.4.1 节操作相同。如果该端口与 1000Base-T 设备相连，相应操作如下：

❶ 当与工作站、服务器或路由器相连时使用CAT5或CAT5E直连网线与交换机前面板的 RJ-45 端口相连（如图 2-11 所示）。当与交换机或中继器相连时使用 CAT5 或 CAT5E 交叉网线。网线的管脚说明参见附录。

❷ 将网线的另一端与所连设备的 RJ-45 端口相连。当交换机与所连设备建立连接之后，相应端口 LED 连接状态指示灯会亮。如果该指示灯不亮，可能是连接设备没开机，连接线路有问题或连接设备的网卡有问题。参考第 6 章解决相关问题。

❸ 如果需要的话，重新配置并重启设备。

❹ 重复 1 至 3 步以将每一个设备连接到 10/100/1000Base-T 端口。

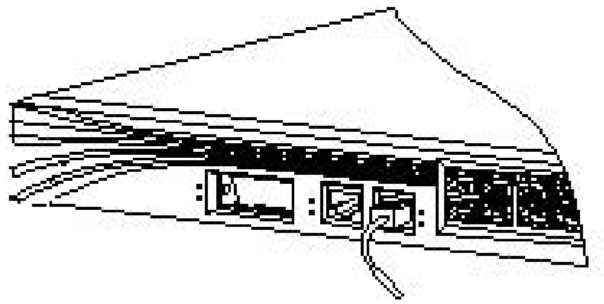


图2-11连接交换机10/100/1000 Base-T端口

2.4.5 1000Base-X GBIC 模块与 10/100/1000Base-T 端口的自动检测、自动切换与容错（只适用于 3524G-L3 交换机）

1000Base-XGBIC模块和与之比邻的10/100/1000Base-T端口可以实现端口的自动检测与自动切换（另一个 10/100/1000Base-T 端口不受影响），他们的工作状态如下表所示。

表 2-1：

	GBIC模块插有可用光纤	GBIC模块没插可用光纤
10/100/1000 Base-T 端口插有可用网线	GBIC模块工作 10/100/1000 Base-T端口不工作	GBIC模块不工作 10/100/1000 Base-T端口工作
10/100/1000 Base-T 端口没插可用网线	GBIC模块工作 10/100/1000 Base-T端口不工作	都不工作

用户可以根据1000Base-X GBIC模块与10/100/1000Base-T端口的自动检测、自动切换的特性将需要连接到交换机上的一台千兆设备同时与这两个端口相连。如果其中一条线路出现问题，交换机会在另一条线路上传输数据以保证该千兆设备正常收发网络数据。

2.4.6 连接交换机控制端口

使用随机提供的专用控制端口电缆将一台PC机或终端与交换机控制端口相连。控制端口和专用电缆的管脚信息参见附录 B。

PC 机或终端必须支持 VT100 终端模拟。终端模拟软件（如 PC 机应用软件 Hyperterminal 等）会在启动程序时建立交换机与 PC 机或终端间的通信。

根据以下步骤将 PC **机或终端连接到交换机上：**

❶ **将随机提供的专用控制端口电缆插入交换机**UART**控制端口如图**2-12**所示。该电缆的管脚信息参见附录** B**。**

❷ **将控制端口电缆的另一端插到所用** PC **的** UART **串口上。**

❸ **如果用户在使用** PC **机或终端，请启动终端模拟程序（超级终端** Hyperterminal)

❹ **配置** PC **机或终端的字符格式，使其与交换机控制端口的以下缺省配置一致。**

波特率：38400
数据位：8
停止位：1
校验：　无

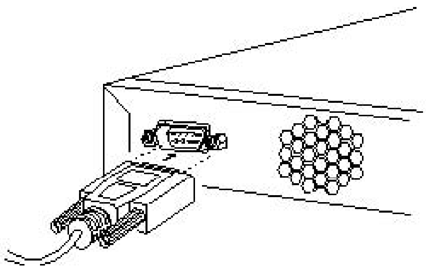


图2-12 ***与交换机控制端口连接***

2.5 Bootrom 启动选项介绍

当交换机上电后，系统进入 Bootrom **启动过程。**Bootrom **启动分为两种方式：自动启动和人工干预启动。下面以** 3524G-L3 **交换机为例说明** Bootrom **启动的两种方式。**

2.5.1 自动启动

在默认方式下，交换机在上电之后，如果用户不干预，交换机等待 3 **秒后直接进入自动启动模式，开始启动映像程序。在等待进入启动模式时的界面如图** 2-13

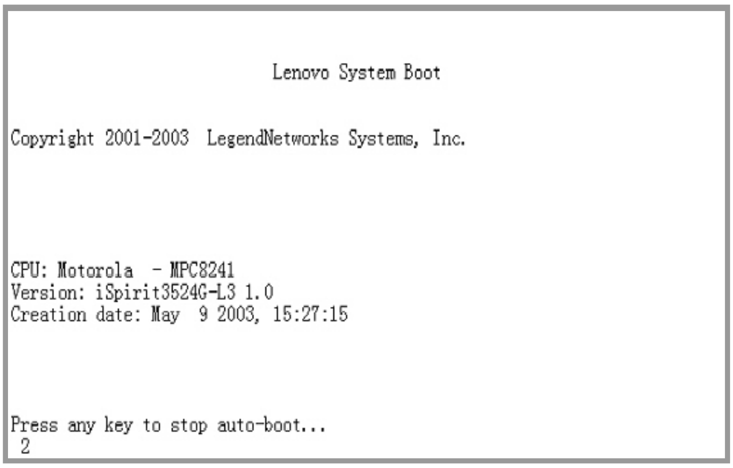


图*2-13 *自动启动模式界面

2.5.2 人工干预启动

在等待进入启动模式的界面下输入除‘@’的任何键后进入 Bootrom 菜单界面，菜单提示符为“[Switch Boot]:”。在该提示符下，支持一些可用的命令，可以输入“？”显示帮助信息，帮助信息如图2-14

```
Press any key to stop auto-boot...
 3

[Switch Boot]: ?

 ?                       - print this list
 @                       - boot (loa                 - print boot params
 c                       - change boot params
                                                   - show/change which boot string i
s active
 boot device: flash                    file name: flash: Lenovo.Z
 Boot flags:
   0x00  - autoboot system image
   0x02  - load local system symbols
   0x04  - don't autoboot
   0x08  - quick autoboot (no countdown)

available boot devices:Enhanced Network Devices
 fei0 flash
[Switch Boot]:
```

图2-14 人工干预启动模式界面

命令的功能

？：显示帮助信息

@**：启动映像程序**

b[<n>]**：显示或改变被激活的模式**

p**：显示启动参数**

c**：设置启动参数**

P**：显示所有** PCI **设备**

2.5.3 通过串口升级 hyper OS

在[Switch Boot]:下输入大写 D 出现 § 后，在超级终端的菜单选择传送，如图 2-15 所示。协议选择 1K XModem，再选择发送即可。

注意：升级时请选用正确的升级文件。

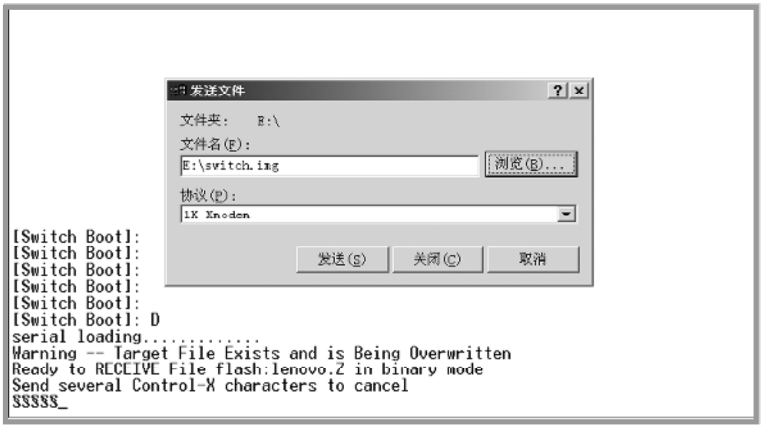


图2-15 通过串口升级hyper OS

2.6 下一步工作

用户可以通过以下方式进一步配置和管理交换机:

1. ANSI/VT100 控制台访问,详细说明参见第 3 章和第 4 章。
2. Web 访问：详细说明参见第 5 章。

第 3 章

CLI 命令行界面管理

本章主要说明以下内容：

1、CLI **命令行界面管理概述**
2、**命令介绍**
3、**命令列表**

3.1 CLI 命令行界面管理概述

3.1.1 模式概述

CLI 命令行接口由 EXEC 模式、CONFIGURATION 模式、VLAN CONFIGURATION 模式、PORT CONFIGURATION 模式、ROUTE CONFIGURATION 模式和 RIP CONFIGURATION 模式组成，每一种模式对应一种命令集。

系统启动后或 telnet 请求后首先进入 EXEC 模式，该模式不需要输入口令，任何用户都可以进入该模式。该模式只有很少的几个命令可用，不能对交换机进行配置。在 EXEC 模式下出现以下命令提示符：

"Switch >"

在 EXEC 模式的提示符 Switch >下输入命令 enable 命令并提供正确的口令进入 CONFIGURATION 模式，CONFIGURATION 模式是管理员才能进入的模式，进入该模式的用户可以完全控制交换机和浏览交换机的状态信息，并且可以对交换机进行配置。该模式有很多命令供用户使用。在 CONFIGURATION 模式下出现以下命令提示符：

"Switch #"

在 CONFIGURATION 模式下执行命令 vlan <vlan-id>进入 VLAN CONFIGURATION 模式，VLAN CONFIGURATION 模式是一个配置子模式，专门用于配置一个特定的 VLAN ID 的模式。VLAN CONFIGURATION 模式的提示符：

"Switch (vlan-1)#"(vlan-id 为 1 时)。

在 CONFIGURATION 模式下执行命令 port <port-number>进入 PORT CONFIGURATION 模式，PORT CONFIGURATION 模式是一个配置子模式，专门用于配置一个特定的端口的模式。PORT CONFIGURATION 模式的提示符是：

"Switch (port-26)#"(port-number 为 26 时)。

在 CONFIGURATION 模式下执行命令 route 进入 ROUTE CONFIGURATION 模式，该模式是配置子模式，是管理与路由相关功能的命令集合。ROUTE CONFIGUATION 模式的提示符是：

"Switch (route-configuration)#"

在 CONFIGURATION 模式下执行命令 RIP 进入 RIP CONFIGURATION 模式，该模式是配置子模式，是配置 rip 协议相关信息的命令,RIP CONFIGURATION 模式的提示符是：

"Switch (Rip configuration)#"

3.1.2 命令概述

3.1.2.1 语法帮助

命令行接口中设置有语法帮助，支持每一级命令和参数的帮助功能。如果您对某个命令的语法不太确定，请输入该命令中您所知道的前面的部分，然后键入" ？ "，系统会提示您下一个命令的信息。您就可以根据提示的命令继续输入命令，直至提示命令为<cr>时，表明命令输入完毕。按回车执行所键入的命令。

例如" show ？" 显示所有 show 命令的第二个词的帮助

如 " ip adrress 198.168.80.1 ？ " 能够询问下一个参数的含义。

3.1.2.2 命令简写

支持命令的前缀匹配功能，用户可以键入很少的的键完成一个命令，

例如 " show switch " 命令可以只键入 " sh sw "

3.1.2.3 命令中的符号

您可能会在命令语法中看到各种符号，这些符号只是说明您该如何输入该命令，但是不是命令本身的一个部分。表 3-1 对这些符号进行了概要说明。

表 3-1：

符号	描述
尖括号< >	尖括号表示该命令的部分必须输入一个参数。例如： Switch# mac address <mac-address>中您必须在<mac-address>那个位置输入一个合法的交换机MAC地址。
中括号[ ]	中括号括起来的部分表示这部分为可选参数，用户可以输入也可以不输入

3.1.2.4命令参数类型

一般以尖括号“< ”“> ”括起来的部分是命令参数，命令参数主要分为以下几个类 型。

IP 地址：	当尖括号内是以下几种类型时，您必须输入一个合法的IP地址：<remote-host>;<ip-address>;<subnet-mask>; <gateway-address>等。
MAC 地址：	<mac-address>
文 件 名 ：	当尖括号中是 file-name 时，表示该参数是文件名。
端 口 速 度 ：	当尖括号中是 speed-value 时，表示该参数是端口的速度。
端 口 列 表 ：	当尖括号中是 port-list 时，表示该参数是端口列表。多个端口之间用空格分开,如果是连续的多个端口可以用该连续端口的最小端口加上减号“ – ”再加上该连续端口的最大端口号表 示 。
时 间 ：	当尖括号中是 age 时，表示该参数是时间，以秒为单位。
端 口 号 ：	当尖括号中是 port-number 时，表示该参数是端口号。
字 符 串 ：	当尖括号为 str 时，表示需要输入的是一个字符串。
接口:	当尖括号为sw时,表示需要输入的是接口号,接口号值为0-31
虚拟子网号：	当尖括号中是vlan-id时,输入虚拟子网号值1-4094。

3.1.2.5 行编辑命令

支持行编辑功能，如 CTRL+U 删除整个命令行，CTRL+H 删除前一个字符等。行编辑常见命令快捷键列表见表 3-2。

表3-2

符号	描述
Ctrl+c	中断
Ctrl+p 或↑键	上一条命令
Ctrl+n 或↓键	下一条命令
Ctrl+u	删除整行
Ctrl+a	光标回到行首
Ctrl+f 或→键	光标向右移动一格
Ctrl+b 或←键	光标向左移动一格
Ctrl+d	删除光标所在的字符
Ctrl+h	删除光标前一个字符
Ctrl+k	删除光标处及光标后的所有字符
Ctrl+x	删除光标处及光标前的所有字符
Ctrl+e	光标移到行尾

注意：“→” “←” “↑” “↓”键只能在 telnet 中使用。

3.1.2.6 用户密码

系统缺省设置了一个用户帐号，用户名是 admin。该用户名用于网页登录。缺省密码是 password。用户进入后可以修改密码。需要输入两次口令，如果两次输入相同才接受此新口令。

3.1.2.7 历史命令使用

支持命令的历史记录功能，能记住用户最近使用的10个历史命令，把用户最近键入的命令保存起来。您可以用 show history 来显示已经输入过的命令，您也可以用 CTRL+P，CTRL+N 或上下键（只有 telnet 可用）来选择历史命令。

3.1.3 功能配置清单

iSpirit 3524G/F-L3 交换机具有以下配置功能：

●基本功能
●端口配置
●二层转发表
●存取配置文件
●系统软件升级
●系统时钟
●系统安全
●VLAN 配置
●STP 协议
●TRUNK功能
●端口镜像功能
●802.1p功能
●广播风暴控制
●流控功能
●GMP监听功能
●DHCP、BOOTP 功能
●论证计费功能
●SNMP 协议
●IP子网设置
●DHCP中继
●静态路由
●ACL 功能
●RIP协议

3.2 功能配置介绍

3.2.1 系统的基本功能

用户可以在 configuration 模式（Switch#）下使用 CLI 命令，这些命令用于维护交换机的通常管理,比如修改密码、显示交换机配置信息等基本功能的管理。

3.2.1.1 系统的基本配置和管理

➢进入系统的CONFIGURATION配置模式

首先在 EXEC 模式(提示符为 Switch>的模式)，执行 enable 指令，输入密码后进入 CONFIGURATION 配置模式(提示符为 Switch# 的模式)，如下所示：

Switch> **enable**

Password：

Switch#

注意:用户输入正确密码并确认后才可进入 CONFIGURATION 配置模式，交换机提供一个缺省密码。

➢设置交换机的IP地址及子网掩码

ip address <ip-address><subnet-mask>

例:Switch# **ip address 192.168.2.3 255.255.255.0**

➢设置交换机的缺省网关

ip gateway <gateway-address>

例：Switch# **ip gateway 192.168.2.1**

➢重新启动计算机

Switch# **reset**

➢ 重新启动计算机，并恢复到出厂模式

Switch# **reset factory**

➢修改交换机口令

Switch# **password**

➢ 把配置信息保存在flash中

Switch# **save**

➢退出配置模式

Switch# **exit**

➢清除屏幕上的所有信息
Switch# **cls**

➢ **测试交换机与远端机器的网络连通性**
Switch# **ping <remote-host>**
例：假设交换机的IP**地址是**198.168.80.1**，有一台直连主机的**IP**地址是**198.168.80. 72**，交换机测试主机的连通性。**
Switch# **ping 198.168.80.72**
连通显示：
PING 198.168.80.72: 56 data bytes
64 bytes from host (198.168.80.72): icmp_seq=0. time=0. ms
64 bytes from host (198.168.80.72): icmp_seq=1. time=0. ms
64 bytes from host (198.168.80.72): icmp_seq=2. time=0. ms
64 bytes from host (198.168.80.72): icmp_seq=3. time=0. ms
64 bytes from host (198.168.80.72): icmp_seq=4. time=0. ms
—— 198.168.80.72 PING Statistics——
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/3/16
未连通显示：
PING 199.168.80.72: 56 data bytes
no answer from 199.168.80.72

➢ **显示最近**10**条历史指令**
Switch# **show history**

➢ **显示交换机的系统信息。系统描述、产品名称、版本信息、启动时间等**
Switch# **show system**

➢ **显示交换机的一些配置信息。**IP **地址、**MAC、IP gateway **和协议的启用情况**
Switch# **show switch**

➢ **显示串口连接参数**
Switch# **show console**

➢ **显示当前会话的终端的宽度和高度（能显示多少个字符）**
Switch# **show terminal**

➢ **显示交换机的** IP **地址信息。**IP **地址，子网掩码、网关**
Switch# **show ip**

3.2.1.2 系统的基本配置和管理命令列表

用户对系统的基本配置和管理命令列表3-3用于维护交换机的通常管理，比如修改密码、显示交换机配置信息等。

表3-3

符号	描述
logout	退出当前的telnet会话
cls	清除屏幕上的所有信息
Exit	不同的模式其功能不一样。EXEC模式：与命令logout相同。CONFIGURATION模式：退出CONFIGURATION模式到EXEC模式。VLAN CONFIGURATION模式：退出VLAN CONFIGURATION模式到CONFIGURATION模式。PORT CONFIGURATION模式：退出PORT CONFIGURATION模式到CONFIGURATION模式。ROUTE CONFIGUATION模式: 退出ROUTE CONFIGURATION模式到CONFIGURATION模式。RIP CONFIGUATION模式: 退出RIP CONFIGURATION模式到CONFIGURATION模式。
enable	进入CONFIGURATION模式，要求输入正确口令。
show console	显示串口控制台的信息，包括波特率，字符个数，检验位，停止位。
ping <remote-host>	测试交换机与远端机器的网络连通性，并把测试结果显示出来
show terminal	显示当前会话的终端的宽度和高度。
show history	显示所有的历史命令。
show console	显示串口控制台的信息，包括波特率，字符个数，检验位，停止位。
ip address <ip address>[<subnet-mask>]	设置交换机的IP地址及子网掩码。
show ip	显示交换机的IP地址及子网掩码及缺省网关信息
show switch	显示交换机的一些配置信息。
show system	显示交换机的一些系统信息。
password	修改进入CONFIGURATION模式的口令。
menu	进入MENU管理模式。
save	把配置信息保存到FLASH中。
reset[<factory>]	重启系统或重启系统并恢复出厂的初始配置
traffic classes	启动traffic classes
no traffic classes	停止traffic classes
show connection	显示交换机的TCP,UDP连接情况。

3.2.2 端口配置功能

用户可以在端口配置模式Switch(port-id)**或管理员配置模式**Switch#**下实现对端口通信数率、优先级、**vid **等设置。**

3.2.2.1 端口的配置和管理过程

用户可以在端口配置模式Switch(port-id)**或管理员配置模式**Switch#**下实现对端口通信数率、优先级、**vid **等设置比如：**

- **进入端口配置模式。**

  Switch# **port <port-number>**

  <port-number>，范围1～26。**例如对交换机的**1 **端口进行配置,<port-number>就表示**1。**如下所示：**

  Switch# **port 1**

  Switch(port-1)#

- **显示交换机某个端口的所有信息。 端口的连接速率、**pvid、STP **状态等。**

  在CONFIGURATION**模式下**

  Switch# **show port <port-number>**

  在PORT CONFIGURATION**模式下**

  Switch(port-1)# **showport**

  如下所示：

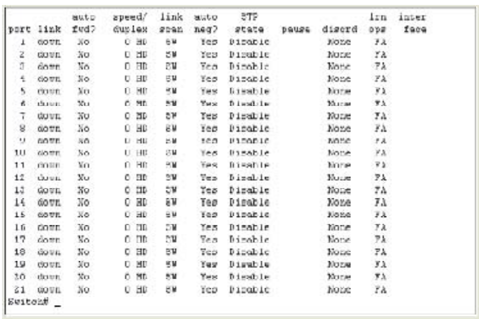
```
Switch# show port 1
 Unit                 : 1
 Port                 : 1
 ifIndex              : 0x2100001
 State                : Enable
 Set Speed            : autonegotiate
 Actual Speed         : unknown
 STP State            : Disabled
 Link                 : Down
 Mac Learn            : Unlock
 Port Vlan ID         : 1
 Port Default Priority : 0
 Drop Events          : 0
 Octets               : 0
 Packets              : 0
```

```
Broadcasts              : 0
 Multicasts             : 0
 CRCAlignErrors         : 0
 UndersizePkts          : 0
 OversizePkts           : 0
 Fragments              : 0
 Jabbers                : 0
 Collisions             : 0
 Pkt64Octets            : 0
 — More —
 Pkts65to127Octets      : 0
 Pkts128to255Octets     : 0
 Pkts256to511Octets     : 0
 Pkts512to1023Octets    : 0
 Pkts1024to1518Octets   : 0
Switch#
```

➢ **显示交换机所有端口的概要信息。端口的连接速率、连接状态。**

Switch# **show port all**

图例 3-1 **显示了输入了 show port all 命令后的结果：**



port	link	auto fvd?	speed/ duplex	link scan	auto neg?	STP state	pause	discrd	lrn ops	inter face
1	down	No	0 HD	SW	Yes	Disable		None	FA	
2	down	No	0 HD	SW	Yes	Disable		None	FA	
3	down	No	0 HD	SW	Yes	Disable		None	FA	
4	down	No	0 HD	SW	Yes	Disable		None	FA	
5	down	No	0 HD	SW	Yes	Disable		None	FA	
6	down	No	0 HD	SW	Yes	Disable		None	FA	
7	down	No	0 HD	SW	Yes	Disable		None	FA	
8	down	No	0 HD	SW	Yes	Disable		None	FA	
9	down	No	0 HD	SW	Yes	Disable		None	FA	
10	down	No	0 HD	SW	Yes	Disable		None	FA	
11	down	No	0 HD	SW	Yes	Disable		None	FA	
12	down	No	0 HD	SW	Yes	Disable		None	FA	
13	down	No	0 HD	SW	Yes	Disable		None	FA	
14	down	No	0 HD	SW	Yes	Disable		None	FA	
15	down	No	0 HD	SW	Yes	Disable		None	FA	
16	down	No	0 HD	SW	Yes	Disable		None	FA	
17	down	No	0 HD	SW	Yes	Disable		None	FA	
18	down	No	0 HD	SW	Yes	Disable		None	FA	
19	down	No	0 HD	SW	Yes	Disable		None	FA	
20	down	No	0 HD	SW	Yes	Disable		None	FA	
21	down	No	0 HD	SW	Yes	Disable		None	FA	

Switch# _

图3-1 显示交换机端口概要信息

- **打开和关闭端口。使配置的交换机端口可用或不可用。**

  在CONFIGURATION**模式下启用端口，可以启用任意端口。**

  Switch# **enable port <port-list1> [<port-list2>] .. [<port-listn>]**

  示例：如果需要启用1-4、8-12**端口，执行如下指令**

  Switch# **enable port 1-4 8-12**

  在PORT CONFIGURATION**模式下启用端口，只启用当前端口**

  Switch(port-1)# **enable**

  在CONFIGURATION**模式下关闭端口，可以关闭任意端口。**

  Switch# **disable port <port-list1> [<port-list2>] .. [<port-listn>]**

  示例：如果需要关闭1-4、8-12**端口，执行如下指令**

  Switch# **disable port 1-4 8-12**

  在PORT CONFIGURATION**模式下关闭端口，只关闭当前端口**

  Switch(port-1)# **disable**

- **配置端口速度。配置交换机端口的速率。在**PORT CONFIGURATION**模式下执行**

  Switch(port-1)# **speed <speed-value>**

  交换机缺省设置是：auto negotiate，

  可以设置的状态：

  autonegotiate　　**端口与端口进行速度自协商**

  full-10/ half-10　　**全双工**10M/**半双工**10M

  full-100/ half-100　　**全双工**100M/**半双工**100M

  full-1000/ half-1000　**全双工**1000M/**半双工**1000M

  示例：将交换机端口1**的连接速率设置成**100M**全双工**

  Switch(port-1)# **speed full-100**

- **设定端口的优先级。可以配置端口转发数据的优先级级别**

  Switch(port-1)# **ppd < Priority-value>**

  缺省 priority-value**：**0

  示例：将交换机端口1**的优先级值设置成**3

  Switch(port-1)# **ppd 3**

  注意：端口优先级按照0-7**的顺序依次增高**

- **设定端口的**pvid。

  Switch(port-1)# **pvid < vlan-number>**

  端口缺省的pvid**：**1

  可以将交换机端口的pvid**改成端口归属的**PVID**号**

  示例：端口1**属于**vlan1~2，pvid**为**1

  Switch# **vlan 2**

Vlan 2 added
Switch(vlan-2)# **port 1**
Switch(port-1)# **pvid 1**

3.2.2.2 端口的配置和管理命令列表

用户可以在端口配置模式Switch(port-id)**或管理员配置模式**Switch#**下通过表**3-4 **中的命令实现对端口通信数率、优先级、**vid **等设置。**

表3-4

符号	描述
show port all	显示交换机所有端口状态的简单信息
show port<portid>	显示交换机上该端口的状态信息
port <port-number>	进入给定的端口号的PORT CONFIGURATION模式
speed <speed value>	设定正在配置的端口的速度。
Pvid <vlan-id>	设置正被配置的端口的PVID。
ppd<priority-number>	设置正被配置的端口的缺省优先级

3.2.3 二层转发表

ARL **是** Address Resolution Logic **的简称，是二层交换机硬件转发数据帧的核心。硬件根据数据帧目的** MAC **地址查找** ARL **表找到相应的表项，并把数据帧送到相应的输出端口。交换机根据数据帧的源**MAC**地址以及发送端口自动学习生成表项。除自动学习外，管理员也能定制** ARL **表项。**ARL **命令就是用于管理** ARL **表的命令。**

3.2.3.1二层转发表的配置和管理

- **向** arl**表中加入一个单播**MAC**地址表项**

  Switch# **arl**

  示例：在port 1**上加入一个单播地址**00:01:23:45:67:89

  Switch# arl
  Mac Address: 00:01:23:45:67:89
  Port Number: 1

VLAN id (1): 1
Switch# arl
MAC Adress **输入添加的** MAC **的地址。**
Port Number **输入添加** MAC **地址对应的端口。**
Static **表示添加的** MAC **地址是否写入硬件表，一般选择** y。

- **向** marl**表中加入一个多播**MAC**地址表项**

  Switch# **marl**
  示例：在port 1**上加入一个多播地址**01:01:23:45:67:89
  Switch# marl
  Mac Address: 01:01:23:45:67:89
  Port Number List: 1
  VLAN id (1): 1
  Entry has been added to MARL table,
  you can use command ‘show marl all’ to get all the entries.
  Switch#
  MAC Adress **输入添加的** MAC **的地址。**
  Port Number List **输入添加** MAC **地址对应的端口。**
  VLAN id（1）**表示添加的组播地址对应的** vlan。

- **设定交换机地址表的老化时间**

  Switch# **agetimer <time-value>**
  缺省设置是：300 **秒。允许设置范围：**10 **秒** =<A<=1000000 **秒。**
  示例：设置交换机的老化时间为 100 **秒**
  Switch# **agetimer 100**
  Switch#

- **显示交换机所有的单播地址信息**

  Switch# **show arl all**

- **显示交换机某些端口的单播地址信息**

  Switch# **show arl ports < port-lists> [<port-list2>] .. [<port-listn>]**
  示例：显示交换机 1-4 **端口的单播地址信息**
  Switch# **show arl ports 1-4**

- **显示单播**MAC**地址对应的信息**

Switch# **show arl mac <MAC address>**

示例：显示单播MAC**地址**00:00:03:01:13:00**对应的信息**

Switch# sh arl mac 000003011300

```
 MAC_ADDR  VLANID  PORT CPU L3 SD_DIS STATIC AGE TID SCP
-----------------------------------------------------------------------------------------
00:00:03:01:13:00    1     1    0  1    0    1    0   0    0
Switch#
```

- **显示交换机所有组播地址的信息**

Switch# **show marl all**

- **显示交换机某些端口的组播地址信息**

Switch# **show marl ports < port-lists> [<port-list2>] .. [<port-listn>]**

示例：显示交换机1-4 **端口的组播地址信息**

Switch# **show marl ports 1-4**

- **显示组播**MAC**地址对应的信息**

Switch# **show marl mac <MAC address>**

示例：显示组播 MAC **地址** 01:00:5e:00:00:01 **对应的信息**

Switch# sh arl mac 01005e000001

```
 MAC_ADDR    LANID COS_DST PORT_BITMAP UT_PORT_BITMAP
 ——————————————————————————————————————————
 01:00:5e:00:00:01   1      0     0xc000000      0x0000000
Switch#
```

- **显示地址表的老化时间**

Switch# **show arl agetime**

- **从** arl **表中删除一个单播** MAC **地址表项**

Switch# **no arl**

- **从** marl **表中删除一个多播** MAC **地址表项**

Switch# **no marl**

3.2.3.2 二层转发表的配置和管理命令列表

表3-5说明了二层转发表的配置和管理命令，

表3-5

符号	描述
arl	向arl表中加入一个表项，包括单播MAC地址表项和多播地址表项。
no arl <mac-address>	从arl表中删除固定的MAC地址的表项。
show arl all	显示arl表中的所有表项
show arl ports <port-list1> [<port-list2>] …… [<port-listn>]	显示arl表中所有给定端口的单播地址表项
marl	向marl表中加入一个多播地址表项
no marl <mac-address>	从marl表中删除给定的多播MAC地址的表项
show marl all	显示marl表中的所有多播地址表项
show arl mac <mac-address>	显示marl表中MAC地址与给定多播MAC地址相同的表项
show arl agetime	显示二层交换表表项超时时间间隔
agetimer <age>	设定表项超时的时间

3.2.4 存取配置文件功能

每次修改交换机的配置后，都要执行save命令。这样配置信息在交换机重新启动后才会继续存在。管理员也可以通过 TFTP 完成配置文件的上传和下载。

3.2.4.1存取配置文件功能的配置和管理

在 CONFIGURATIONA 模式下，可以将交换机的配置文件进行备份，上传配置文件的指令：

Switch# **upload configuration <IP address> <Name>**

IP address：表示文件上传目的 PC 的 IP 地址。

Name： 表示配置文件的命名。

下载配置文件的指令：

Switch# **download configuration <IP address> <Name>**

IP address：表示文件上传目的 PC 的 IP 地址。

Name： 表示配置文件的命名。

操作步骤如下：

第一步：搭建备份文件需要网络环境

第二步：将交换机配置信息生成配置文件；

第三步：将配置文件备份到 PC（备份过程已经完成，必要时，进行下一步操作 ）

第四步：将配置的备份文件重新下载到交换机。

示例：一台已经配置了 vlan 和接口地址的交换机，需要进行配置文件备份。

第一步：搭建如图 3-2 所示网络环境

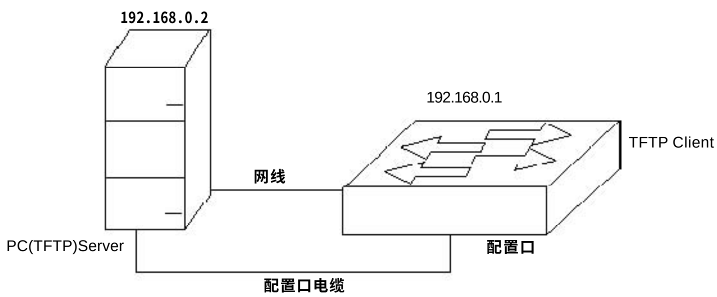


图3-2 存取配置文件功能的搭建网络环境

配置备份文件需要的网络环境过程:将交换机的配置口通过电缆外接一台配置终端，并通过网线与一台 PC 相连。在 PC 安装 TFTP Server，配置 PC 的以太网口 IP 地址，假定 PC 的 IP 地址为 192.168.0.2。然后，配置交换机以太网口 IP 地址，假定交换机的 IP 地址为 192.168.0.1。

注意:

微机网口IP地址与交换机以太网口IP地址应位于同一网段。运行TFTP Server，为备份的配置文件指明路径：首先，运行 TFTP Server。TFTPD32 窗口界面如图 3-3 ：

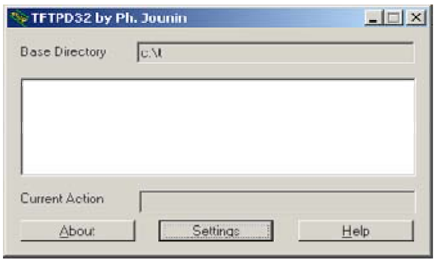


图3-3 TFTPD32界面图

然后，设置备份配置文件的目录。具体操作是，单击[Settings]按钮，出现 TFTPD32 设置界面，如图 3-4。

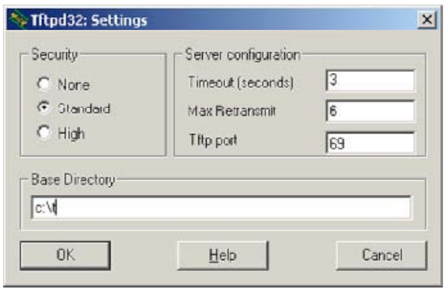


图3-4 TFTPD32设置界面图

在上图所示的“ Base Directory ”下方的空白方框中输入文件路径。单击[OK]按钮确认。

第二步：将交换机的配置信息生成配置文件

在交换机任意管理模式下执行 save **指令，就可以将配置信息生成配置文件。**

第三步：将文件备份到 PC **上**

Switch# **upload configuration 192.168.0.2 beifen**

uploading configuration ......

complete

Switch#

第四步：必要时，将备份文件下载到交换机

Switch# **download configuration 192.168.0.2 beifen**

Do you wish to continue? [Y/N]: y

downloading configuration ......

Complete.

Switch# **reset**

Do you wish to continue**？是询问操作是否继续进行。**Y **表示是；**N **表示否。**

3.2.4.2 存取配置文件功能的配置和管理命令列表

表3-6**说明了存取配置文件功能的配置和管理的命令**

表3-6

符号	描述
save	把配置信息保存到FLASH中。
upload configuration<ip-address><file-name>	把交换机FLASH中的配置文件上载到计算机中保存起来。
download configuraion<ip-address><file-name>	把计算机上的配置文件下载到FLASH中

3.2.5 交换机系统软件升级功能的配置和管理

iSpirit 3524G/F-L3交换机软件版本支持在线升级。升级是通过工具TFTP来完成的 。

3.2.5.1 交换机系统软件升级功能的配置和管理过程

在 configuration 模式下，可以将交换机的映像文件升级，指令如下：

Switch# **download image <ip-address> <file-name>**

其中<ip-address>为PC机的IP地址,<file-name>为在PC机上映像程序文件名。

升级映像文件步骤：

1、搭建升级环境

第一步：搭建升级环境。如下图所示。

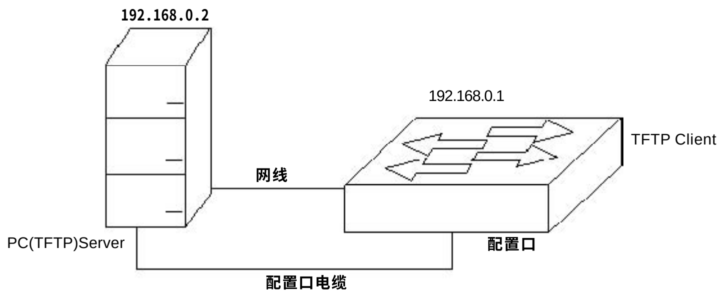


图3-5 搭建TFTP升级环境

第二步:将交换机的配置口通过电缆外接一台配置终端。

第三步：在微机上安装 TFTP Server；

第四步：将新的映像文件拷贝到某一路径下，假定路径为 C:\t；

第五步：配置微机的以太网口 IP 地址，假定微机的 IP 地址为 192.168.0.2。

第六步：配置交换机以太网口 IP 地址，假定交换机的 IP 地址为 192.168.0.1

注意：微机网口 IP 地址与交换机以太网口 IP 地址应位于同一网段。

2、运行 TFTP Server

第一步：运行TFTP Server。TFTPD32 **窗口界面如下图：**

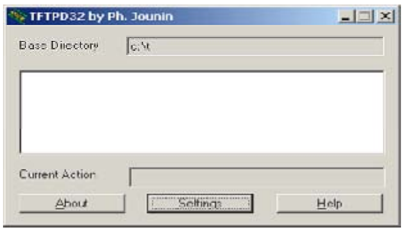


图3-6 TFTPD32界面图

第二步：设置TFTP Server**文件目录。启动**TFTP Server**之后，重新设置**TFTP Server**文件目录，将待加载的映像文件拷贝到此目录之中。具体操作是，在图**3-6**所示的页面中单击**[Settings]**按钮，出现**TFTPD32 **设置界面如图**3-7。**在“**Base Directory **”中输入文件路径。单击**[OK]**按钮确认。**

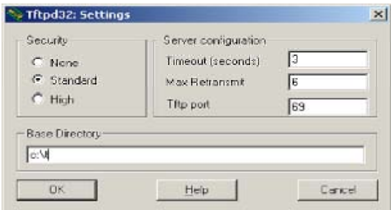


图3-7 TFTPD32设置界面图

3、配置交换机

第一步：连接交换机，选择以太网接口后，将该接口与运行TFTP Server **程序的微机通过以太网线连接。并用**ping**命令检测微机交换机是否连通。**

第二步：在超级终端 Switch# **中输入命令：**

Switch# download image 192.168.0.2 iSpirit3524G2V10.img，**回车，等待出现**complete **字样时下载映像文件完毕，如下所示：**

Do you wish to continue? [Y/N]: y

downloading image......

Complete.

Switch#

注意：交换机升级过程中不能断电。

第三步：重新启动交换机。

Switch# **reset**

3.2.5.2 交换机系统软件升级功能的配置和管理命令列表

表3-7说明了交换机系统软件升级功能的配置和管理命令，

表3-7

符号	描述
download image<ip-address><file-name>	用于应用程序映像版本的更新，用户可以用此命令把在计算机上的最新程序映像下载到交换机的FLASH中

3.2.6 系统时钟

3524G/F-L3 交换机具有实时时钟，用户可以通过命令来设置和显示时钟。

3.2.6.1 系统时钟的配置和管理

系统时钟可以依以下步骤进行配置和管理：

➢ **配置交换机系统时钟**

Switch# **settime**

示例：将交换机的系统时间设置成 04 **年** 1 **月** 1 **日** 13 **时** 5 **分** 30 **秒**

Switch# **settime**

Year (0-99) : 04

Month (1-12) : 1

Day (1-31) : 1

Hour (0-23) : 13

Minute (0-59) : 5

Second (0-59) : 30

➢ **显示交换机系统时钟**

Switch# **gettime**

示例：显示交换机系统时间

Switch# gettime

13:05:3001/01/2004

3.2.6.2 系统时钟的配置和管理命令

表3-8说明了系统时钟的配置和管理命令

表3-8

符号	描述
gettime	获得系统时钟
settime	设置系统时钟

3.2.7 系统安全功能

iSpirit系列交换机对于安全的管理可以控制到不同的级别。可以锁定端口不再学习新的地址；可以实现端口和 mac 地址的绑定，一个端口最多可以绑定 128 个 mac 地址；若是通过 ACL、802.1x 可以实现更加安全的管理。

3.2.7.1 系统安全功能的配置和管理

系统安全可依据以下步骤进行配置和管理

- MAC地址与端口绑定功能实现

  Switch# **mac bind**

  示例：将00:01:5c:de:45:7d 绑定在端口 1 上

  Switch# mac bind

  Mac Address : 00:01:5c:de:45:7d

  Port Number : 1

  VLAN id : 1

- 删除MAC地址与端口的绑定

  Switch# **no mac bind**

  示例：将绑定的 MAC 地址 00:01:5c:de:45:7d 删除

  Switch# no mac bind

  Mac Address : 00:01:5c:de:45:7d

  Port Number : 1

  VLAN id : 1

  Switch#

- 端口锁定功能的实现。此指令在PORT CONFIGURATION模式下执行

  Switch(port-1)# **lock**

  执行此指令以后，当前端口就被锁定，不能学习新的 MAC 地址。

➢ **取消端口锁定功能。此指令在**PORT CONFIGURATIONM**模式下执行**
Switch(port-1)# **unlock**

3.2.7.2 系统安全功能的配置和管理命令

表3-9**说明了系统时钟的配置和管理命令**

表3-9

符号	描述
mac bind	具体的MAC地址和端口号进行绑定
no mac bind	解除该端口与MAC地址的绑定
lock <port-list1> [<port-list2>] …… [<port-listn>]	锁定给定的端口不学习新的MAC地址
unlock <port-list1> [<port-list2>] …… [<port-listn>]	解锁定给定的端口，使它们能够学习新的MAC地址
lock	锁定正被配置的端口，不学西新的MAC地址
unlock	解锁定正被配置的端口，使它们能够学习新的MAC地址
enable	使正被配置的端口可用
disable	使正被配置的端口不可用
enable ports<port-list1> [<port-list2>] …… [<port-listn>]	使给定的端口可用
disable ports <port-list1> [<port-list2>] …… [<port-listn>]	使给定的端口不可用

3.2.8 VLAN 的配置和管理

VLAN（Virtual Local Area Network）即虚拟局域网，是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段，从而实现虚拟工作组的新兴技术。任何一个端口的集合（甚至交换机上的所有端口）都可以被看作是一个 VLAN。VLAN 的划分不受硬件设备物理连接的限制，用户可以通过命令灵活的划分端口，创建 VLAN。

VLAN 可以限制广播数据广播的范围。假设在 VLAN " 市场部 " 中的一个设备发出一个广播报文，那么只有" 市场部 "这个VLAN中的设备才能收到该广播报文，其它部门不能收到该广播报文。VLAN可以提供更高的安全性。正常情况每个设备只能与在同一 VLAN 中的设备通信，不能直接访问。如果 VLAN 之间设备要相互通信只能通过三层路由才能实现。VLAN可以简化设备在网络中的移动带来的管理。因为VLAN是从逻辑划分的，当一个用户移动物理位置时，它还可以属于原来的VLAN。这样就不需改变原来的配置。

3524G/F-L3支持基于端口Vlan的划分。这种划分是把一个或多个交换机上的几个端口划分一个逻辑组，这是最简单、最有效的划分方法。该方法只需网络管理员对网络设备的交换端口指定 VLAN 即可，不用考虑该端口所连接的设备。IEEE802.1Q规定了依据以太网交换机的端口来划分VLAN的国际标准。使不同厂商的设备可以同时在一个网络中使用，各自的 VLAN 设置可以被其他设备所识别，实现互通。根据 IEEE802.1Q，端口可以标志 Tagged 和 Untagged，Tagged/Untagged 标志该端口所连接的设备是否能够支持带有802.1Q Tag header的帧。3524G/F-L3交换机一个端口可以属于多个 Tagged VLAN ID 和多个 Untagged VLAN ID。VLAN ID 的范围为 1 到 4094，交换机最多支持 256 个 VLAN。

3.2.8.1 VLAN的配置和管理过程

交换机的 vlan 设置分为以下几个步骤：
第一步：创建一个 vlan
第二步：将端口添加到相应 vlan 当中

- **创建 vlan，在任何操作模式下都可以执行如下指令**
  Switch# **vlan <vlan-id>**
  注意：VLAN-id 的范围是 1~4094

- **进入 vlan 设置模式，向 vlan 中添加成员**
  向某一个 vlan 添加 untag 成员以前，需要进入 vlan 设置模式
  Switch# **vlan <vlan-id>**

向 vlan **中添加的端口可以是** vlan **的** tag **成员，也可以是** vlan **的** untag **成员**,**向** vlan **中添加** tag **成员，指令如下**

Switch(vlan-2)# **tag <port-list1> [<port-list2>] .. [<port-listn>]**

向 vlan **中添加** untag **成员，指令如下**

Switch(vlan-2)# **untag <port-list1> [<port-list2>] .. [<port-listn>]**

示例：在 vlan2 **中添加** untag **成员端口** 5-8，tag **成员端口** 9-12

Switch# vlan 2

Vlan 2 added

Switch(vlan-2)# untag 5-8

Switch(vlan-2)# tag 9-12

- **在** vlan **中禁止使用某些端口。在** VLAN CONFIGURATION **模式下执行**
  Switch(vlan-2)# **forbidden <port-list1> [<port-list2>] .. [<port-listn>]**
  示例：在 vlan2 **中禁用** 13-16 **端口**
  Switch(vlan-2)# **forbidden 13-16**

- **从** vlan **中删除端口。在** VLAN CONFIGURATION **模式下执行**
  从 vlan **中删除** tag **成员**
  Switch(vlan-2)# **no tag <port-list1> [<port-list2>] .. [<port-listn>]**
  从 vlan **中删除** untag **成员**
  Switch(vlan-2)# **no untag <port-list1> [<port-list2>] .. [<port-listn>]**
  示例：在 vlan2 **中删除** untag **成员端口** 5-8，tag **成员端口** 9-12
  Switch# vlan 2
  Switch(vlan-2)# no untag 5-8
  Switch(vlan-2)# no tag 9-12

- **显示交换机的** vlan **信息。在** VLAN CONFIGURATION、CONFIGURATION **模式下执行**
  Switch# **show vlan**

- **显示每个** vlan **的详细信息。在** VLAN CONFIGURATION、CONFIGURATION **模式下执行**
  Switch# **show vlan <vlan-id>**

- **删除** vlan。**在** CONFIGURATION **模式下运行**
  Switch# **no vlan <vlan-id>**

3.2.8.2 vlan 典型配置实例（基于 PORT 的 VLAN）

1、在单台交换机上配置

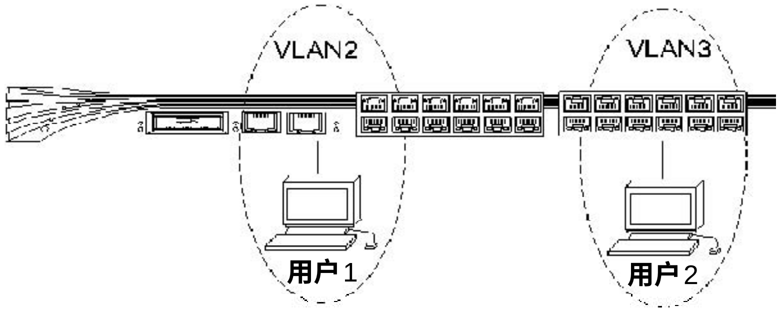


图3-8 基于PORT 的VLAN 示意图

如上图所示，有两个用户，用户 1 **和用户** 2**，两个用户由于所使用的网络功能和环境不同，需要分别处于不同的** VLAN **中。用户** 1 **在** VLAN2**，连接交换机的端口** 2**，用户** 2 **在** VLAN3**，连接端口** 3。**需要在交换机上做如下设置：**

```
Switch# vlan 2
 Vlan 2 added
Switch(vlan-2)#exit
Switch# vlan 3
Vlan 3 added
Switch(vlan-3)# vlan 2
Switch(vlan-2)# untag 2
Switch(vlan-2)# vlan 3
Switch(vlan-3)# untag 3
Switch(vlan-3)#exit
Switch# port 2
Switch(port-2)# pvid 2
Switch(port-2)# port 3
Switch(port-3)# pvid 3
```

2. 跨交换机配置 VLAN

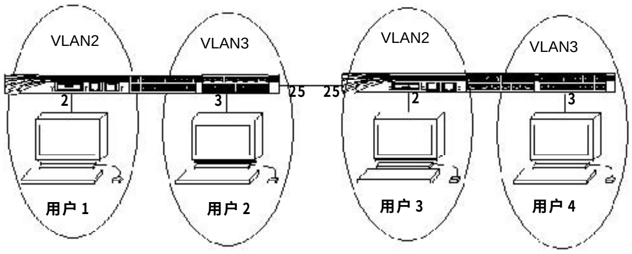


图3-9 802.1Q的vlan配置

图3-9显示两台交换机分别连接两个用户，表3-10列出了两台交换机分别连接两个用户的配置需求

表3-10

客户名称	连接的交换机	连接交换机端口	所属vlan	级联端口
用户1	交换机1	1	Vlan 3	25
用户2	交换机1	2	Vlan 2	
用户3	交换机2	1	Vlan 3	25
用户4	交换机2	2	Vlan 2	

根据以上图示和表格中的配置要求，需要在两台交换机上做配置，具体的配置步骤如下所示：

交换机 1 的配置步骤：

```
witch# vlan 2
 Vlan 2 added
Switch(vlan-2)# untag 2
Switch(vlan-2)# tag 25
Switch(vlan-2)# exit
Switch# vlan 3
 Vlan 3 added
Switch(vlan-3)# untag 3
Switch(vlan-3)# tag 25
Switch(vlan-3)# exit
Switch# port 2
Switch(port-2)# pvid 2
Switch(port-2)# exit
Switch# port 3
Switch(port-3)# pvid 3
Switch(port-3)# exit
```

交换机2 **的配置步骤：**

```
witch# vlan 2
 Vlan 2 added
Switch(vlan-2)# untag 2
Switch(vlan-2)# tag 25
Switch(vlan-2)# exit
Switch# vlan 3
 Vlan 3 added
Switch(vlan-3)# untag 3
Switch(vlan-3)# tag 25
Switch(vlan-3)# exit
Switch# port 2
Switch(port-2)# pvid 2
Switch(port-2)# exit
Switch# port 3
Switch(port-3)# pvid 3
Switch(port-3)# exit
```

3.2.8.3 VLAN配置常见问题分析及解决方式

3.2.8.3.1 在单台交换机上配置VLAN的常见问题分析及解决方式

如果配置后，发现不同VLAN**之间的**PC**机不能通信，那是正常现象，因为不同**VLAN**之间要进行通信，必须要经过三层的路由转发。**

如果同一VLAN**内的**PC**机不能进行通信，须作以下验证：**

1**、查看整体有哪些**VLAN

```
Switch# show vlan
————————————————————————————
|VID |Name                | Status |
|——+———————————————————+————|
|1   |Default VLAN 1       | Static |
|——————————————————————————|
|2   |vlan2               | Static |
|——————————————————————————|
|3   |vlan3               | Static |
|——————————————————————————|
```

2.**查看连接特定**PC**机的端口是否在那个**VLAN**内，并且是以**"U"**的形式加入的**

```
Switch# show vlan 2
Vlan ID:        2
Vlan Name:      vlan2
Vlan Status:    Static
                  (-=None, M=Member, F=Forbidden, U=Untagged)
--------------------------------------------------------------------
| PortNumber |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|2|2|
|            |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|
|------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
|Configuration|-|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
--------------------------------------------------------------------

Switch# show vlan 3
Vlan ID:        3
Vlan Name:      vlan3
Vlan Status:    Static
                  (-=None, M=Member, F=Forbidden, U=Untagged)
--------------------------------------------------------------------
| PortNumber |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|2|2|
|            |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|
|------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
|Configuration|-|-|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
--------------------------------------------------------------------
```

3.**查看那个特定的端口，端口的**pvid**号必须和端口所在**vlan**的号码一致**
例如，端口2 **在** vlan 2 **中，端口**2 **的** pvid **号为** 2 **。**

```
Switch# show port 2
 Unit               :  1
 Port               :  2
 ifIndex            :  0x2100002
 State              :  Enable
 Set Speed          :  autonegotiate
 Actual Speed       :  unknown
 STP State          :  Disabled
 Link               :  Down
 MacLearn           :  Unlock
 PortVlanID         :  2
 PortDefaultPriority :  0
 DropEvents         :  0
```

```
Switch# show port 3
 Unit              :  1
 Port              :  3
 ifIndex           :  0x2100003
 State             :  Enable
 Set Speed         :  autonegotiate
 Actual Speed      :  unknown
 STP State         :  Disabled
 Link              :  Down
 MacLearn          :  Unlock
 PortVlanID        :  3
 PortDefaultPriority :  0
 DropEvents        :  0
```

3.2.8.3.2 跨交换机配置VLAN的常见问题及分析方式

跨交换机的 vlan**，在同一个** vlan **内的** pc **机都能够通信，如果不能相通，须查看如下：**

1 **、连接** pc **机的端口是以"** U **"模式加入这个** VLAN **的，并且端口的** pvid **号和** vlan **号应该一致。**

2 、级联端口是加入到每一个 vlan **中的，并且在每一个** vlan **内都是以"** M **"模式加入的，并且端口的** PVID **号为** 1**。**

```
Switch# show vlan

______________________________________________
|VID |Name                      | Status |
|----+---------------------------+--------|
|1   |Default VLAN 1             | Static |
|-----------------------------------------|
|2   |vlan2                      | Static |
|-----------------------------------------|
|3   |vlan3                      | Static |
|-----------------------------------------|
```

注意：每个交换机的端口 2 **的** pvid **号为** 2**，端口** 3 **的** pvid **号为** 3**，级联端口** 25 **的** pvid **还是为** 1

3.2.8.4 VLAN命令列表

表3-11 说明了VLAN配置命令

表3-11

符号	描述
vlan<vlan-id>	进入此VLAN ID的VLAN CONFIGURATION模式。若该VLAN ID不存在，创建该VLAN ID
no vlan<vlan-id>	从VLAN表中删除给定的VLAN ID。
show vlan[<vlan-id>]	显示所有的或某个特定的VLAN信息。
tagged <port-list1> [<port-list2>] …… [<port-listn>]	设定给定的端口为正配置的VLAN的 tagged成员
no tagged<port-list1> [<port-list2>] …… [<port-listn>]	取消给定的端口为正配置的VLAN的 tagged成员
untagged<port-list1> [<port-list2>] …… [<port-listn>]	设定给定的端口为正配置的VLAN的 untagged成员。
no untagged<port-list1> [<port-list2>] …… [<port-listn>]	取消给定的端口为正配置的VLAN的 untagged成员。
forbidden<port-list1> [<port-list2>] …… [<port-listn>]	禁止给定的端口为正配置的VLAN的成员。
no forbidden<port-list1>...	取消禁止给定的端口为正配置的VLAN的成员。
name <vlan-name>	修改正配置的VLAN的名字。

3.2.9 STP 协议的配置和管理

联想天工iSpirit 3524G-L3/3524F-L3 交换机支持IEEE802.1d标准的STP 协议。STP 是运行在 Bridges 和 Switches 层上，符合 IEEE802.1d 协议标准兼容的第二层协议。这一协议提供了网络的动态冗余切换机制。因此使用 STP，可以让您在网络设计中部署备份线路，并且保证在主线路正常工作时，备份线路是关闭的。当主线路出现故障时，自动激活备份线路，将数据流切换到备份线路，保证设备正常运行。

由此可见，使用 STP，可以保证当在网络结构上存在冗余路径情况下，阻止网络回路发生。网络回路对网络来说是致命的打击，冗余链路作为网络备份路径又是非常重要的。通过交换机提供的命令可以实现该协议的功能。

3.2.9.1 STP协议的配置过程

交换机的 STP 功能配置分以下几个步骤：
第一步：启用 STP 协议；
第二步：对 STP 参数进行设置；

- 打开或关闭 STP：
  switch# stp <enable/disable> 或 no stp

- 使能 STP 端口，使端口用于 STP 计算
  switch# enable stp ports <port-list1>[<port-list2>…[<port-listn>]

- 关闭 STP 端口，使端口不用于 STP 运算
  switch# disable stp ports <port-list1>[<port-list2>…[<port-listn>]

- 使能正在配置的 STP 端口，使端口用于 STP 计算
  switch(port-2)# stp port enable

- 关闭正在配置的 STP 端口，使端口不用于 STP 计算
  switch(port-2)# stp port disable

- 设置桥优先级，其默认值为 32768。
  switch# stp bridge priority
  说明：priority 的范围为 0~65535。0 的优先级最高，65535 的优先级最 低 。

➢ **设定端口优先级，其默认值为**128**。**
switch# stp port priority
说明：priority 的范围为 0~255。0 的优先级最高，255 的优先级最低。

➢ **设置桥的**BPDU**报文发送周期，默认值为**2**秒。**
switch# stp bridge hello-time

➢ **设置**STP**的转发延迟时间，默认值**15**秒。**
switch# stp bridge forward-delay

➢ **设置桥的**STP**配置信息的最大存活时间，默认值为**20**秒。**
switch# stp bridge max-age

➢ **显示某个端口信息**
switch# show stp port<port-number>

3.2.9.2 STP典型配置实例

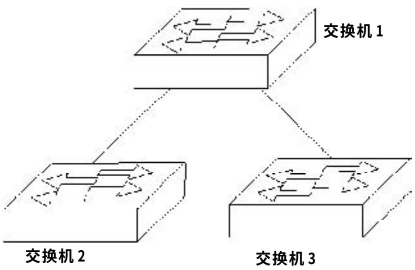


图3-10 STP配置

三台交换机连接成一个环状,因为生成树协议是默认打开的,所以不需要打开生成树协议。

如果需要打开每一台交换机的生成树协议,分别在每一台交换机上执行

Switch# stp enable <cr>

确认生成树协议在每一台交换机上是打开的

```
Switch# show switch
 Ip Address        : 192.168.0.1
 Subnet Mask       : 255.255.255.0
 Default Gateway   : 0.0.0.0
 MAC Address       : 00:09:ca:01:75:02
 BOOTP             : Disable
 DHCP              : Disable
 Spanning Tree     : Enable
```

IGMP Snooping : Enable
Reset : no reset
DhcpRelay : Disable

这样生成树协议就能正常运行

如果需要关闭生成树协议的运行，需要输入命令

Switch# stp disable

生成树协议的高级命令：

设置其中第一台交换机为根交换机,需要设置他的桥优先级比其他两个桥的优先级要小，默认优先级为32768

Switch# stp bridge priority A stp bridge priority (0=<A<=65535)

使交换机的某个端口不参与生成树的运行,需要关闭端口的生成树功能

Switch# disable stp ports A-B or A port list (1=<A,B<=8)

3.2.9.3 配置stp的常见问题分析及解决方式

察看哪一个交换机被选为根网桥:

Switch# show stp bridge

— Designated Root Information —-
Priority : 32768
MAC Address : 00:09:ca:01:75:02 **（根网桥配置状态）**
Hello Time : 2s
Forward Delay : 15s
Max Age : 20s

— Bridge STP Information —-
Bridge Priority : 32768
MAC Address : 00:09:ca:01:75:02 **（本网桥配置状态）**
Root Path Cost : 0
Root Port : 0
Bridge Hello Time : 2s
Bridge Forward Delay : 15s
Bridge Max Age : 20s

察看生成树中交换机的端口状态：

Switch# show stp port A port number (1=<A<=8)

Switch# show stp port 1
— Port Information —-
STP Port : Enable

Port ID : 1
Priority : 128
State : Disabled
Path Cost : 19
Designated Cost : 0

— Designated Root Information —-
Priority : 32768
MAC Address : 00:09:ca:01:75:02

— Designated Port Information —-
Port ID : 1
Priority : 128
— Designated Bridge Information —-
Priority : 32768
MAC Address : 00:09:ca:01:75:02

3.2.9.4 STP命令列表

表3-12说明了STP配置命令列表

表3-12

符号	描述
stp	在交换机上启动stp协议
no stp	在交换机上关闭stp协议
show stp bridge	显示stp和本交换机的桥信息
stp port disable	关闭正在配置的stp端口，使端口不用于stp计算
stp port enable	使能正在配置的stp端口，使端口用于stp计算
stp port priority <priority-number>	设置端口优先级
show stp port <port-number>	显示某个端口的stp信息，包括本端口，指定根，指定桥，指定端口的信息
stp bridge hello-time <interval>	设置桥的hello time
stp bridge forward-delay <interval>	设置桥的forward delay
stp bridge max-age <interval>	设置桥的max age

3.2.10 TRUNK 功能

Port Trunking 技术是一种将网络流量聚集在一组端口上的方法,以形成一个交换机之间的大容量的通道或容错的通道。通道之间可以实现流量均衡。联想天工 iSpirit 3524G-L3/3524F-L3 交换机支持Port Trunking,通过创建Port Trunking 来提升交换机之间的带宽。Port Trunking把多个物理端口捆绑在一起当作一个逻辑端口来使用。如果 Port Trunking 中的一个端口发生堵塞或故障，那么数据包会被重新分配到该 Port Trunking 中的别的端口进行传输。如果这个故障端口重新恢复正常，那么数据包将重新分配到该Port Trunking 中的所有端口进行传输。联想天工iSpirit 3524G-L3/3524F-L3 交换机的Port Trunking 功能与Intel 和Cisco 的同类产品的Port Trunking 功能兼容。

3.2.10.1 TRUNK功能的配置和管理过程

交换机的 Trunk 功能配置分以下几个步骤：

第一步：创建 Trunk 组

第二步：修改 trunk 组的参数

- 创建一个Port Trunking组

  Switch# Trunk

  在这个交互操作中依次输入 tid <0-5> 、rtag <1-6>、port list

注 意 ：

本产品支持六个聚合。每个聚合支持八个10/100M端口聚合或两个10/100/1000M的端口聚合在一起。这是一个交互式命令，首先输入 trunk Id 号，接着输入 rtag 号，端口聚合的方法它的值为 1-6，1：基于源 MAC 地址；2：基于目的 MAC 地址；3：基于源和目的 MAC 地址一起；4：基于源 IP 地址；5：基于目的 IP 地址；6：基于源和目的 IP 地址一起来决定输出端口。总共有六种可能。最后输入 trunk ports 列表 。

示例:将 1-3 端口设置到 Tid 是 2 的 Rtag 是 5 的 trunk 组

```
Switch# trunk
trunk_Id:  2
trunk_Rtag:  5
ports_list:  1-3
```

- 取消 Trunk 组

  Switch# no trunk <tid>

- 显示 Trunk 配置

  Switch# show trunk

- **修改已经配置的**trunk**组的聚合方式**
  Switch#trunk rtag <tid> <Rtag>

- **修改已经配置的**trunk**组的端口成员**
  Switch#trunk ports <tid> <port list>

- **删除已经配置的**trunk**组的成员**
  Switch#trunk no ports <tid> <port list>

- **将指定的**trunk**组端口加入到组播组中**
  Switch#trunk mcast
  在交互操作下依次输入tid**以及组播地址和**vid
  示例:**将**trunk**组加入到组播组中**
  Switch# trunk mcast
  trunk_Id: 2
  Mac Address: 01:00:5e:11:11:11
  Vlan ID: 1

- **恢复** trunk**到缺省设置**
  Swtich#trunk table init

3.2.10.2 TRUNK功能的典型配置

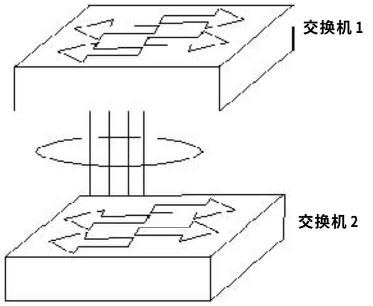


图3-11 TRUNK功能典型配置

如图所示需要配置交换机1和交换机2之间做trunk链路，各自捆绑1-4端口做链路聚合时需要在每个交换机上执行以下命令：

Switch# trunk <cr> set trunk configuration
Switch# trunk
trunk_Id: 1 trunk 的 ID 号
trunk_Rtag: 1 trunk 的 tag 号
ports_list: 1-4 **加入 trunk 组的端口号**

注意：做 trunk 时，两边交换机的端口数量要一致，速度、双工等端口参数都要完全一致,但不必两边的端口号一一对应。

删除一个trunk组

Switch# no trunk A trunk indentifier(0<=tid<=5)

删除所有的trunk组

Switch# trunk table init <cr>

3.2.10.3 trunk 配置时常见的问题及解决方式

如果 trunk **没有起作用，需要查看以下状态**

Switch# show trun

TGID	RTAG	status	Ports
0	0	Not_ready	0x00000000(none)
1	**1**	**Active**	**0x0000001e(fe1-fe4)**
2	0	Not_ready	0x00000000(none)
3	0	Not_ready	0x00000000(none)
4	0	Not_ready	0x00000000(none)
5	0	Not_ready	0x00000000(none)

注意：加入 trunk **组的几个端口一定要属于同一个** vlan**，速率，双工等端口属性都要设置一样。**

3.2.10.4 Trunk命令列表

表3-13**说明了**Trunk**命令列表**

表3-13

符号	描述
show trunk	显示聚合表中所有聚合的信息，如哪些端口聚合在一起以及聚合的方法
trunk table init	初始化聚合表信息，清空聚合表
trunk	把给定的端口聚合在一起
no trunk <tId>	取消聚合,命令后跟trunk Id 号
trunk rtag <tId><method>	修改聚合方法
trunk ports <tId> <portlist>	向某个存在的聚合中添加端口
trunk no ports <tId> <portlist>	向某个存在的聚合中删除端口
trunk mcast	它把一个trunk项加入到一个存在的多播地址中

3.2.11 端口镜像功能

交换机端口镜像功能就是用户将所有的流量从一个特定的端口复制到一个指定的镜像端口，以便进行流量和协议分析。这样，这些流量就可以被一个特殊的设备监控。它对发现和修理故障有很大的帮助。

联想天工iSpirit 3524G-L3/3524F-L3 交换机能够分别侦听端口的进入数据和出去数据，还可以决定是侦听同一个VLAN的数据包还是不同VLAN的数据包。一个侦听端口可以同时侦听多个端口。

3.2.11.1 端口镜像功能的配置和管理

iSpirit 3524G/F-L3交换机可以有一个镜象端口，端口镜像功能的配置和管理包含交换机的 mirror 设置包括设置 mirror、删除 mirror、察看 mirror 信息。

- 创建一个mirror

  Switch# mirror

  示例：通过镜像，使用端口 10 侦听 1-5 端口的流入和流出流量(L2 模式)。

  Switch# mirror

  Mirror Mode: l2

  Mirror Port: 10

  Egress ports_list: 1-5

  Ingress ports_list: 1-5

  说明:Mirror port 为镜像端口，Egress port表示输入被侦听数据进入端口的数据流，Ingress port 表示被侦听数据出端口的数据流。
- 删除mirror设置

  Switch#no mirror
- 察看交换机的mirror设置信息

  Switch#show mirror

  示例:如下拓扑图，要求捕获 pc 同 FTP server 之间通信的会话。

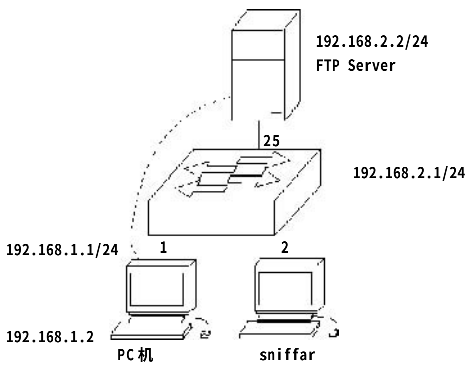


图3-12拓扑示意图

实现步骤：

1 、**在**3524G**上创建相应的**Vlan**和子网**

Switch# vlan 2
Vlan 2 added
Switch(vlan-2)# untag 1
Switch(vlan-2)# vlan 3
Vlan 3 added
Switch(vlan-3)# untag 2
Switch(vlan-3)# ex
Switch# route
Switch(route-config)# ip subnet
Netware Interface: 1
Agent Ip Addr: 192.168.1.1
Net Mask: 255.255.255.0
Vlan ID: 2
Interface Descript:
Switch(route-config)# ip subnet
Netware Interface: 2
Agent Ip Addr: 192.168.2.1
Net Mask: 255.255.255.0
Vlan ID: 3
Interface Descript:

2、**将** 3524G **的端口** 1 **镜像到端口** 2 **上启用镜像，将端口** 2 **作为监控端口**

Switch# mirror
Mirror Mode: l2
Mirror Port: 2
Egress ports_list:1
Ingress ports_list:1

3.2.11.2 端口镜像功能的典型配置实例及常见问题分析解决

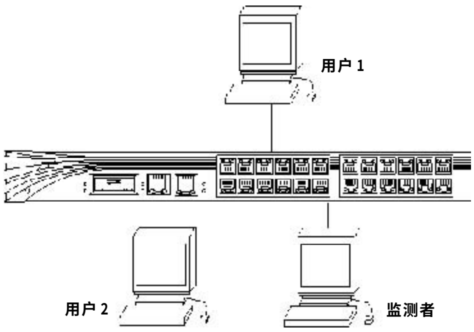


图3-13 端口镜像配置

在如上图所示的环境下需要在一台交换机中，用户1**和用户**2**正在通信，正常情况下其他端口的用户是无法获取其通信信息的,为了检测数据流是否正常,监测者需要获取其数据流，就要用到端口镜像问题 。用户** 1 **连接到端口** 1**，用户** 2 **连接到端口**2**,监测者连接在端口**8**,使监测者能够捕捉到其数据流可以做以下两种配置监测用户有 1 或用户 2：**

通过监测用户1**的流量**

Switch# mirror
Mirror Mode: L2
Mirror Port: 8
Egress ports_list: 1
Ingress ports_list: 1

或通过监测用户2**的流量**

Switch# mirror
Mirror Mode: L2
Mirror Port: 8
Egress ports_list: 2
Ingress ports_list: 2

3.2.11.3 配置端口镜像功能时常见的问题及解决方式

在配置端口镜像功能时需要确保镜像配置正确:

不要把镜像端口和被镜像端口搞反了。

镜像端口是mirror ports,**指的是观测端口**

被镜像端口是Egress ports , Ingress ports , **指的是被观测端口**

用show mirror **命令进行确认**

```
Switch# show mirror
Mirror Mode: L2
Mirror Port: 8
Egress ports_list: 1
Ingress ports_list: 1
```

3.2.11.4 端口镜像功能的命令列表

表3-14 **说明了**Trunk**命令列表**

表3-14

符号	描述
show mirror	显示交换机端口侦听设置信息
mirror	设置端口侦听信息
no mirror	取消交换机端口侦听设置信息

3.2.12 802.1p功能

802.1p定义了优先级的概念，在MAC桢头增加3位优先级指明该数据包优先级。这样，对于那些实时性要求很高的数据包，可以赋予高的优先级，当以太网交换机数据流量比较多时，它会考虑优先转发这些优先级高的数据包。联想天工iSpirit 3524G-L3/3524F-L3 交换机提供4个优先级队列与802.1p的优先级匹配，为多媒体或其他数据流提供灵活的端口优先级机制。

3.2.12.1 802.1p功能的配置和管理

802.1p功能的配置过程包含802.1p包含定义优先级对应的服务优先队列、每个端口支持的服务优先队列的个数,以及查看相关信息的指令。

- 设置802.1p 的8 个优先级对应的服务优先级队列
  Switch#cos map
  注意：这是一个交互式命令，要求用户指定802.1p 的8 个优先级各自对应的服务优先级队列，队列0 优先级最高，3 的优先级最小。

- 设置每个端口支持的服务优先级队列个数
  Switch#cos maxnum
  注意：这个值可以为1 ，2 ，4

- 显示802.1p 的8 个优先级各自对应的服务优先级队列
  SwitcH#show cos map

- 显示支持的服务类别的个数命令
  Switch#show cos maxnum

3.2.12.2 802.1p功能的配置命令列表

表3-15说明了802.1p命令列表

表3-15

符号	描述
cos map	设置802.1p的8个优先级对应的服务优先级队列
cos maxnum	设置每个端口支持的服务优先级个数
show cos map	显示802.1p的8个优先级各自对应的服务优先级

3.2.13 广播风暴控制功能

支持广播风暴控制作用是限制每个端口单位时间连续广播信息包的数量,每个广播信息包被存储到缓存器然后,一个一个地被转发到其它端口,当被存储的数目超过允许个数时,设备将丢弃连续到来的广播信息包。联想天工iSpirit 3524G-L3/3524F-L3 交换机支持对于广播的控制，同时支持多播的控制。这个功能可以避免广播使网络阻塞，减轻 CPU 的负担。

3.2.13.1 广播风暴控制功能的配置和管理

广播风暴控制功能的配置过程包含设置交换机的广播和多播包限制以及显示限制端口限制广播和多播的配置情况(默认情况下此功能是关闭的)。

- **设置端口风暴抑制**

  示例:

  Switch#storm

  Limit:1500

  Bcast(y/n):y

  Mcast(y/n):n

  DLF(y/n):y

- **显示限制端口限制广播和多播的配置情况**

  Switch#show storm

  Current settings ：

  Limit = 1500

  Bcast = True

  Mcast = Fasle

  DLF = True

3.2.13.2 广播风暴控制功能的命令列表

表3-16说明了广播风暴控制功能命令列表

表3-16

符号	描述
storm-control	设置每个端口每秒可以接收的广播和多播数据包的个数

3.2.14 流控功能

流量控制用于防止在端口阻塞的情况下丢帧。在半双工方式下,流量控制是通过背压（Backpressure）技术实现的，使得信息源降低发送速度。在全双工方式下流量控制一般遵循IEEE 802.3x标准,阻塞的端口向信息源发送“Pause”帧令其暂停发送。iSpirit 3524G/F-L3 还支持线端阻塞（HOL）预防机制，发生阻塞时，收到“ Pause”帧的端口并不降低向别的端口发送数度。

3.2.14.1 流控功能的配置和管理

流控功能的配置包含设置端口支持或者不支持流控、设置端口支持或者不支持防止线端阻塞的配置

- **设置某些端口支持流控**
  Switch#flow control <port-list1> [<port-list2>] .. [<port-listn>]

- **设置正配置端口支持流控**
  Switch(port-1)#flow control

- **设置端口不支持流控**
  Switch#no flow control <port-list>

- **设置正配置端口不支持流控**
  Switch(port-1)#no flow control

- **设置某些端口支持防止线端阻塞**
  Switch#hol prevention <port-list>

- **设置正在配置的端口支持防止线端阻塞**
  Switch(port-1)#hol prevention

- **设置某些端口不支持防止线端阻塞**
  Switch#no hol prevention <port-list>

- **设置正配置端口不支持防止线端阻塞**
  Switch(port-1)#no hol prevention

3.2.14.2 流控功能的命令列表

在 iSpirit 3524G/F 交换机的流控功能中含有以下命令，如表3-17

表3-17

符号	描述
flow control	设置正配置支持流控
no flow control	设置正配置不支持流控
hol prevention	设置某些端口支持防止线端阻塞
no hol prevention	设置正配置不支持防止线端阻塞

3.2.15 IGMP监听功能

IGMP组播成员管理机制是针对第三层设计的,在第三层路由器可以对组播报文的转发进行控制。但是在很多情况下组播报文要不可避免地经过一些二层交换设备,尤其是在局域网环境里如果不对二层设备进行相应的配置则组播报文就会转发给二层交换设备的所有端口这显然会浪费大量的系统资源，IGMP 监听（IGMP Snooping）可以解决这个问题。主机发出 IGMP 成员报告消息，这个消息是给路由器的，IGMP 成员报告经过交换机时，交换机对这个消息进行监听并记录下来，形成多播地址和端口的对应关系,交换机在收到组播数据报文时,根据多播地址和端口的对应关系仅向具有该多播地址对应的端口列表转发组播报文。IGMP监听可以解决二层环境中的组播报文泛滥问题，但需要占用 CPU 处理时间。

3.2.15.1 IGMP监听功能的配置和管理

IGMP 监听功能的配置和管理包含启动、停止 Igmp snooping 以及显示 Igmp snooping信息

- **启动**igmp snooping

  Switch#igmp snooping

- **停止**igmp snooping

  Switch#no igmpsnooping

- **显示**igmp snooping

  Switch#showigmpsnooping

3.2.15.2 IGMP监听功能的命令列表

在 iSpirit 3524G/F 交换机的 IGMP 监听中含有以下命令，如表3-18

表3-18

符号	描述
igmp snooping	启动igmp snooping
no igmpsnooping	停止igmp snooping
igmp snooping age	设置age时间
igmp snooping immeditate-leave	允许组播成员立即离开
no igmp snoopingimmeditate-leave	关闭组播成员立即离开功能
show igmpsnooping	显示igmp snooping信息

3.2.16 DHCP、BOOTP 功能

通过 DHCP、BOOTP 功能交换机可以实现从远端获得 ip 地址的能力。

3.2.16.1 DHCP、BOOTP 功能的配置和管理

- 使能 DHCP 协议
  Switch#dhcp

- 关闭 DHCP 协议
  Switch# no dhcp

- 设置 dhcp server 的 ip 地址功能
  Switch#dhcp server <ipaddr>

- 显示 dhcp server 的 ip 地址
  Switch#showdhcpserver

- 启动 bootp 协议
  Switch#bootp

- 停止 bootp 协议
  Switch#no bootp

3.2.16.2 DHCP、BOOTP 功能的命令列表

表 3-19 说明了在 iSpirit 3524G/F 交换机的 DHCP、BOOTP 监听功能中含有的命令。

表3-19

符号	描述
bootp	启动bootp 协议。
no bootp	停止bootp 协议。
dhcp	启动dhcp协议。
no dhcp	停止dhcp 协议。

3.2.17 认证计费功能

来自于传统计算机网络的以太网本身是基于开放的网络系统,目前大量采用的宽带接入服务器和PPPoE方式还存在一些问题。802.1x协议虽然源于IEEE 802.11无线以太网（EAPOW），但它在以太网中的引入，解决了传统的PPPOE和WEB/PORTAL认证方式带来的问题，消除了网络瓶颈，简轻了网络封装开销，降低了建网成本。要实现802.1x认证和计费功能，在网络中必须包含三类设备：客户端、认证系统、认证服务器。

客户端系统:一般为一个用户终端系统,该终端系统通常要安装一个客户端软件,用户通过启动这个客户端软件发起802.1x协议的认证过程。为支持基于端口的接入控制,客户端系统需支持EAPOL（Extensible Authentiation Protocol Over Lan）协议。

认证系统：通常为支持802.1x协议的网络设备（如以太网交换机）。该设备对应于不同用户（可以是物理端口，也可以是用户设备的MAC地址、VLAN、IP等）有两个逻辑端口：受控（controlled Port）端口和不受控端口（uncontrolled Port）。不受控端口始终处于双向连通状态,可保证客户端始终可以发出或接受认证。受控端口只有在认证通过的状态下才打开,用于传递网络资源和服务。受控端口可配置为双向受控、仅输入受控两种方式,以适应不同的应用环境。如果用户未通过认证,则受控端口处于未认证状态，则用户无法访问认证系统提供的服务。

认证服务器：通常为RADIUS服务器，该服务器可以存储有关用户的信息，比如用户所属的VLAN、CAR参数、优先级、用户的访问控制列表等等。当用户通过认证后,认证服务器会把用户的相关信息传递给认证系统,由认证系统构建动态的访问控制列表,用户的后续流量就将接受上述参数的监管。认证服务器和RADIUS服务器之间通过EAP协议进行通信。

联想天工网络提供了包括客户端、认证系统、认证服务器一套可管理、可运营的解决方案。联想天工802.1x客户端软件可运行在win9x、windows XP，windows 2000等操作系统上,实现与认证系统的通信,并发起ip地址请求。联想天工iSpirit 3524G-L3/3524F-L3交换机实现了认证系统,一个端口可以支持75个用户的认证和管理,同时实现了嵌入在交换机机上的认证服务器,它支持一千个用户认证,实现包月认证方式,管理员可以使这个认证服务器,也可以连接远端的认证服务器,实现更完善的认证和计费功能。

3.2.17.1 认证计费功能的配置和管理

认证计费功能的配置和管理包含802.1x**设置和认证服务器设置**

- **启动**802.1x **协议**
  Switch#dot 1x

- **关闭**802.1x **协议**
  Switch#no dot 1x

- **设置**802.1x **协议的参数为缺省参数**
  Switch#dot1x default

- **设置交换机与客户端发送请求包时没有响应应重新发送请求包的次数**
  Switch#dot1x max-req <number>

- **设置列表中的交换机端口为协议自动认证端口**
  Switch#dot1x control auto <port list>
  说明：只有通过认证用户才能获得网络资源。
  该命令只有在协议启动后才有效。

- **设置当前配置的交换机端口为协议自动认证端口**
  Switch(port-1)dot1x control auto
  说明：只有通过认证用户才能获得网络资源。
  该命令只有在协议启动后才有效。

- **设置列表中的交换机端口为协议强制认证端口**
  Switch#Control force-authorized <port list>
  说明：不用通过认证也能获得网络资源。
  该命令只有在协议启动后才有效。

- **设置当前配置的交换机端口为协议强制认证端口**
  Switch(port-1)#dot1x control force-authorized
  说明：不用通过认证也能获得网络资源。
  该命令只有在协议启动后才有效。

- **设置列表中的交换机端口为协议强制非认证端口**
  Switch#dot1x control force-unauthorized <port list>
  说明：不能获得网络资源。

- **设置当前配置的交换机端口为协议强制非认证端口**
  Switch(port-1)dot1x control force-unauthorized
  说明: 不能获得网络资源。
  该命令只有在协议启动后才有效。

- **设置启动重新认证机制**
  Switch#dot1x reauth
  说明: 只有在协议启动后才有效。

- **关闭重新认证机制**
  Switch#no dot1x reauth
  说明:只有在协议启动后才有效

- **设置当用户认证失败时，等待用户重新认证时间**
  Switch#dot1x timeout quiet-period <time>
  说明：该命令只有在协议启动后才有效。以秒为单位。

- **设置当用户通过认证后，开始重新认证时间间隔**
  Switch#dot1x timeout re-authperiod
  说明：该命令只有在协议启动后才有效。以秒为单位。

- **设置当给用户发**request /identify **数据时没有响应，等待多长时间重新发包**
  Switch#dot1x t imeout tx-period
  说明：该命令只有在协议启动后才有效。以秒为单位。

- **设置当给服务器发数据包没有响应，等待多长时间重新发包**
  Switch#dot1x timeout server-timeout
  说明：该命令只有在协议启动后才有效。以秒为单位。

- **设置当客户端发**eapol start **时,若没有获得回应，等待多长时间重新发送**
  Switch#dot1x timeout supp-timeout
  说明: **该命令只有在协议启动后才有效。以秒为单位。**

- **设置一个端口支持的用户连接个数**
  Switch(port-1)#dot1x support-host <number>
  说明:**该命令只有在协议启动后才有效。**

- **显示当前**do t1 x **协议相关的配置信息**
  Switch#show dot1x

- **设置**radius **服务器的**ip **地址**
  Switch#radius-server host <ip addr>

- **设置**radius **备用服务器的**ip **地址**
  Switch#radius-server option-host <ip addr>

- **设置与**radius **服务器通讯的**udp **端口号**
  Switch#radius-server udp-port <udp port number>

- **设置**radius **服务器的软件信息**
  Switch#radius-server key <string>
  Switch#radius-server vsa <string>

- **设置与**radius **服务器通讯时的**nas-portnum
  Switch#radius-server attribute nas-portnum <>

- **设置与**radius **服务器通讯时的**nas-porttype
  Switch#radius-server attribute nas-porttype <>

- **设置与**radius **服务器通讯时的**service-type
  Switch#radius-server attribute service-type <>

- **设置与**radius **服务器通讯时的**service-type
  Switch#radius-server attribute service-type <>

- **显示**radius **服务器的设置信息**
  Switch#show radius-server

- **配置交换机为主认证服务器**
  Switch#radius-server host local

- **添加一个用户**
  Switch#user add
  说明：这是一个交互式命令，首先添加用户名，接着添加密码，最后为日期期限.

- **删除一个用户**
  Switch#user delete <用户名>

- **修改一个用户资料**
  Switch#user modify
  说明：这是一个交互式命令

- **显示该用户的用户资料命令**
  Switch#user show <用户名>

- **设置与**radius **服务器通讯时的**service-type
  Switch#radius-server attribute service-type <>

- **显示**radius **服务器的设置信息**
  Switch#show radius-server

- **配置交换机为主认证服务器**
  Switch#radius-server host local

- **添加一个用户**
  Switch#user add
  说明：这是一个交互式命令，首先添加用户名，接着添加密码，最后为日期期限.

- **删除一个用户**
  Switch#user delete <用户名>

- **修改一个用户资料**
  Switch#user modify
  说明：这是一个交互式命令
- **显示该用户的用户资料命令**
  Switch#user show <用户名>

3.2.17.2 认证计费功能的配置命令列表

在 iSpirit 3524G/F 交换机的认证计费功能中含有以下命令，如表3-20

表3-20

符号	描述
dot1x	启动802.1x协议
no dot1x	关闭802.1x协议
dot1x default	设置802.1x协议的参数为缺省参数
dot1x max-req <number>	设置交换机与客户端发送请求包时没有响应应重新发送请求包的次数
dot1x control auto <port list>	设置列表中的交换机端口为协议自动认证端口。只有通过认证用户才能获得网络资源
dot1x control force-authorized <port list>	设置列表中的交换机端口为协议强制认证端口。不用通过认证也能获得网络资源。
dot1x control force-unauthorized <port list>	设置列表中的交换机端口为协议强制非认证端口。不能获得网络资源
dot1x reauth	设置启动重新认证机制
no dot1x reauth	设置关闭重新认证机制
dot1x timeout quiet-period <time>	当用户认证失败时，等待用户重新认证时间
dot1x timeout re-authperiod	当用户通过认证后，开始重新认证时间间隔
dot1x timeout tx-period	当给用户发request/identify数据时没有响应，等待多长时间重新发包
dot1x timeout server-timeout	给服务器发数据包没有响应，等待多长时间重新发包
dot1x timeout supp-timeout	当客户端发eapol start时,若没有获得回应，等待多长时间重新发送
show dot1x	显示当前dot1x协议相关的配置信息
radius-server host <ip addr>	设置radius 服务器的ip地址
radius-server option-host <ip addr>	设置radius 备用服务器的ip地址
radius-server udp-port <udp port number>	设置与radius服务器通讯的udp端口号
radius-server key <string>	设置交换机与radius服务器共享的密码
radius-server vsa <string>	设置radius服务器的软件信息
radius-server attribute nas-portnum <>	设置与radius服务器通讯时的 nas-portnum
radius-server attribute service-type <>	设置与radius服务器通讯时的 service-type
radius-server attribute nas-porttype <>	设置与radius服务器通讯时的 nas-porttype
show radius-server	显示radius服务器的设置信息
radius-server host local	配置交换机为主认证服务器
user add	添加一个用户
user delete <username>	删除一个用户
user modify	修改一个用户资料
user show <username>	显示该用户的用户资料

3.2.18 SNMP 协议

目前，数据通信网络中使用得最广泛的网络管理协议是 SNMP（Simple Network Management Protocol，简单网络管理协议）。它是被广泛接受并投入使用的工业标准,其目标是保证管理信息在任意两点中网络上的任何节点检索信息、进行修改、寻找故障、诊断故障、规划容量和生成报告。它采用轮询机制，提供最基本的功能集，适合小型、快速、低价格的环境使用。它建立在无确认的传输层协议 UDP 上，受到许多产品的支持。目前联想常用的网管平台有 Hyper Manager 和 Hyper View。

管理模型实际上由以下 3 个要素组成：如下图 3-14 所示。

1. 一个或多个网络管理设备，每个都含有网络管理站（Network Management Station—NMS）；
2. 一个或多个被管理的网络设备，每个都含有一个代理（Agent）；
3. 被管理对象的 MIB 库。

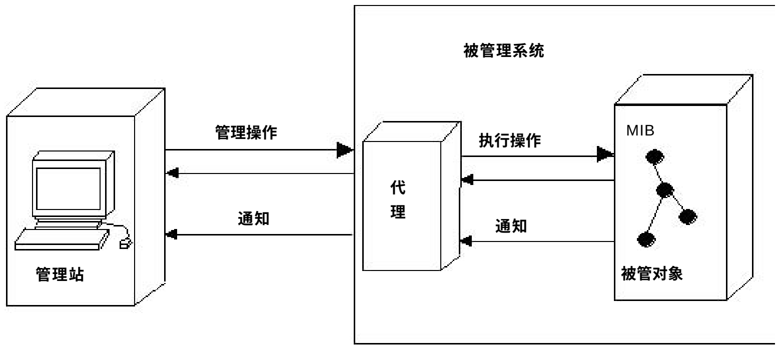


图3-14 网络管理模型

SNMP 允许以下的活动：

1. 一个管理站可以从代理上读取管理信息。（读取管理信息的实际机制取决于代理所支持的 SNMP 的版本号。
2. 一个管理站可以改变或者设定代理上的管理信息。
3. 一个代理可以在没有管理站请求的情况下，向管理站发送信息。这个操作在 SNMPv1 中叫做陷阱(trap)，而在 SNMPv2 中被称作通知(notification)。
4. 陷阱或者通知功能将向管理站报告代理系统中发生的变化。代理必须经过预先的设置，才能知道向何处发送陷阱或者通知。
5. SNMP 向Agent 发出的信息请求中带有一个community 名称(community name)，一个 community 名称类似一个密码。
6. 它必须在管理站上被正确地接收，代理才能存取信息。您必须告知 NNM 您

3.2.18.1 SNMP协议的配置和管理

SNMP 协议的配置和管理包含 snmp trap、snmp commulity 以及 Rmon 设置指令：

- 添加或修改snmp trap 发送的目标
  Switch#snmp trap
  说明：这是一个交互式命令，参数 trap name 是唯一的，如果输入了已经存在的 name，则可以修改这个 trap 目标的配置；参数 Target ip addr 是 trap 发送目标的 ip 地址；参数 version 是消息处理模式，即以哪一种版本的形式发送 t rap。版本 1 值为 1,版本 2 值为 2,版本 3 值为 3。本系统可以设置 8 个 trap 目标项。

- 显示所有的trap 配置
  Switch#show snmp trap

- 删除名字为指定的trap项
  Switch#no snmp trap < trap-name >

- 修改指定的trap 项的目标ip地址
  Switch#snmp trap ip < trap-name > < ip-address >

- 修改名字为t rap-name 的trap项的目标端口
  Switch#snmp trap port < trap-name > < port >

- 修改指定的trap项的重发次数为retries 次
  Switch#snmp trap retries < trap-name > < retries >

- 修改名字为trap-name 的trap 项的发送超时为timeout
  Switch#snmp trap timeout < trap-name > < timeout >
  说明:Timeout 单位是 1/100 秒。

- 修改名字为t rap-name 的t rap 项的消息处理模式
  Switch#snmp trap version <t rap-name> <version>

- 添加或修改访问本交换机的snmp 代理的共用体
  Switch#snmp community
  说明：这是一个交换式命令，参数 Community name 是共用体名称；view name 是访问区域，现在仅支持 internet、Permission 访问权限。本系统一共可以设置 8 个共用体名称。

- **添加或修改trap**
  Switch#snmp trap
  说明：这是一个交换式命令，参数trap name **是用户定义的**trap**名称**Trap Ip Addr **是**trap**报文发送的目的地，**Version**是定义**trap**报文的版本信息。**

- **显示所有**snmp community **的所有配置**
  Switch#show snmp community

- **删除指定的共用体**
  Switch#no snmp community <community-name>

- **添加或修改一个**rmon **事件配置**
  Switch#rmon event [index]
  说明: **这是交互式命令，参数**event type **是发送事件的形式，**1**：** none 2**：**log 3**：**snmp-trap 4**：**log-and-trap**；参数**event owner **是事件属主；参数**Descript ion**是事件描述。如果输入**index **参数则可以添加或修改指定索引的**event **选项。**

- **显示**rmon **事件配置**
  Switch#show rmon configuration event [index]
  说明：如果输入index **参数则可以显示指定索引的**event **选项。**

- **显示发生了**rmon **事件**log
  Switch#show rmon table event

- **删除一个**rmon**事件配置**
  Switch#no rmon event <index>

- **添加或修改一个**rmon **报警配置**
  Switch#rmon alarm [index]
  说明：参数 Interval **为间隔时间，单位秒；参数**Variable **是被检测的数据源，它的类型为**INTEGET、Counter、Gauge **或**TimeTicks**；参数**SampleType **为取样方法，**1 **表示**absoluteValue，2 **表示**eltaValue，**参数**DeltaValue **为触发报警的方式，** 1 **表示**risingAlarm，2 **表示**fallingAlarm，3 **表示**risingOrFallingAlarm**；参数**isingThreshold **为上限阀值；参数**RisingEventIndex **表示当超过上限产生报警时，触发的事件索引；参数**FallingThres hold **为下限阀值；参数**Falling Event Index**为当低于下限产生报警时，触发的事件索引；参数**AlarmOwner **为报警属主；如果输入**index，**则可以添加或修改指定索引的**rmon **报警配置。**

- **显示**rmon **报警配置**
  Switch#show rmon configuration alarm [index]
  说明：如果输入 index **参数则可以显示指定索引的** alarm **选项。**

- **删除一个**rmon **报警配置**
  Switch#no rmon configuration alarm

- **显示** rmon**历史的数据表**
  Switch#show rmon table history

- **显示统计组的数据**
  Switch#show rmon table statistics [index]
  说明：如果输入 index **参数，则可以显示指定索引的** statistics **数据。**

3.2.18.2 SNMP协议的配置实例

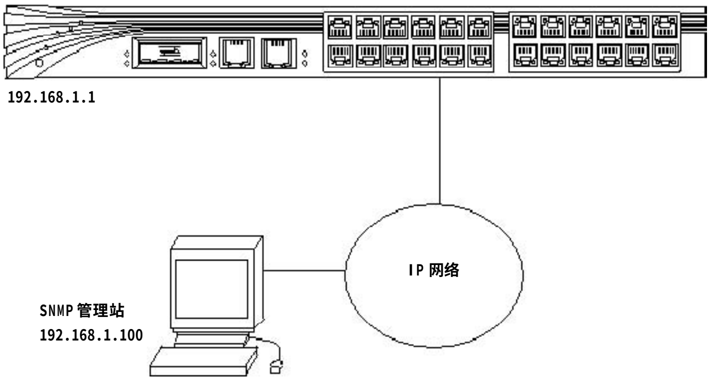


图3-15 SNMP协议配置

如上图环境下，如要在一个SNMP **管理站上面运行** SNMP **管理软件，管理站的** IP **地址为** 192.168.1.100**，被管理的其中一台交换机的** IP **地址为** 192.168.1.1**。交换机和管理站之间并不需要在同一个** IP **网段，只需要之间** IP **能够相互通信，则需要做以下配置：**

在交换机上打开 SNMP**，并且配置** snmp **的** community **，**
只读为 public
读写为private
Switch# snmp community
Community Name : public
View Name(internet) :
ReadOnly(1),ReadWrite(2)
Permission : 1

```
Switch# snmp community
Community Name : private
View Name(internet) :
 ReadOnly(1),ReadWrite(2)
Permission : 2
```

查看 snmp community **的配置**

```
Switch# show snmp community
CommunityName       ViewName                Permission   Status
public              internet                ReadOnly     Active
private             internet                ReadWrite    Active
```

可选配置 trap **指的是当交换机发生特殊情况时，主动向** snmp **管理站发送** snmp **信息需要配置** trap **功能，选择** snmp **版本为** 2

```
Switch# snmp trap
trap name : test
Target Ip Addr: 192.168.1.100
 snmpv1(1),snmpv2(2),snmpv3(3)
Version : 2
```

查看配置信息：

```
Switch# show snmp trap
----------------------------------------------------------------
 Trap Name          : test
 Transport Domain : 1.3.6.1.6.1.1
 Target ip          : 192.168.1.100
 Target port        : 162
 TimeOut            : 1500
 Retry Count        : 0
 Tag List           : rfc1493 rfc1757 rfc1907 rfc2233 tmscom
 Version            : snmp V2
 Storage Type       : nonvolatile
 Status             : Active

----------------------------------------------------------------
```

如果 snmp **不起作用，需要查看以下几个方面**

1 、交换机上需要配置读写或只读的community **，例如只读为**pubic **，读写为**private

2 、需要在 snmp **服务器上配置同样的** community。**才能够** snmp **服务器对交换机进行远程察看或者管理**

如果交换机不能主动发起trap信息给snmp服务器，需要查看以下：

1、交换机上需要配置读写或只读的community,例如只读为pubic,读写为private

2、需要在交换机上设置trap 接收者的ip地址，也就是snmp服务器的ip地址

3、确保交换机的ip地址和snmp服务器之间的ip是能够相通的

3.2.18.3 SNMP协议的命令列表

表3-21含有配置和管理iSpirit 3524G/F-L3交换机的SNMP协议功能命令。

表3-21

符号	描述
snmp trap	添加或修改snmp trap 发送的目标
show snmp trap	显示所有的trap 配置
no snmp trap < trap-name >	删除名字为trap-name的trap项
snmp trap ip < trap-name > < ip-address >	修改名字为trap-name的trap项的目标ip地址为ip-address
snmp trap port < trap-name > < port >	修改名字为trap-name的trap项的目标端口为port
snmp trap retries < trap-name > < retries >	修改名字为trap-name的trap项的重发次数为retries次
snmp trap timeout < trap-name > < timeout >	修改名字为trap-name的trap项的发送超时为timeout。Timeout单位是1/100秒。
snmp trap version <trap-name> <version>	修改名字为trap-name的trap项的消息处理模式
snmp community	添加或修改访问本交换机的snmp代理的共用体名称
show snmp community	显示所有snmp community的所有配置
no snmp community <community-name>	删除一个名字为community-name的共用体名称
rmon event [index]	添加或修改一个rmon 事件配置
show rmon configuration event [index]	显示rmon事件配置
show rmon table event	显示发生了rmon事件log
no rmon event <index>	删除一个rmon事件配置
rmon alarm [index]	添加或修改一个rmon报警配置
show rmon configuration alarm [index]	显示rmon报警配置
no rmon configuration alarm	删除一个rmon报警配置
show rmon table history	显示rmon历史的数据表
show rmon table statistics [index]	显示统计组的数据

3.2.19 ip子网设置

不同VLAN之间的流量不能直接跨越VLAN的边界，需要使用路由，通过路由将报文从一个VLAN转发到另外一个VLAN。联想天工iSpirit 3524G-L3/3524F-L3交换机可以将不同VLAN配置为虚拟的路由接口，从而实现三层数据的转发，通过三层路由功能在不同VLANs间进行相互访问。在建立一个子网时需要指定：接口ID、VLAN ID、子网IP地址、网络掩码、子网名称等信息。

3.2.19.1 ip子网的配置和管理

子网的配置和管理包含子网地址的添加和删除

- 设置交换机的IP地址及子网掩码
  Switch#ip address <ipaddress>[<subnetmask>]

- 设置交换机的缺省网关
  Switch#ip gateway<gatewayaddress>

- 显示交换机的IP地址及子网掩码及缺省网关信息
  Switch#show ip

- 给指定的子网和vlan添加一个网络接口地址
  Switch(route-config)#ip subnet
  说明：该命令是一个交互式命令，要求用户输入接口号，接口IP地址，子网掩码，vlan Id，描述信息。

- 删除交换机一个子网接口
  Switch(route-config)#no ip subnet <ipaddr>

- 显示交换机子网接口信息
  Switch(route-config)#show ip subnet table

3.2.19.2 ip子网的配置实例

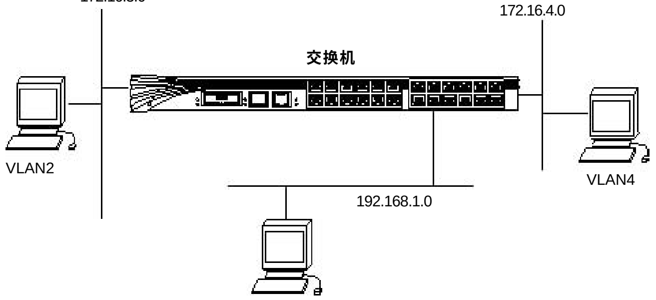


图3-16 ip子网的配置实例

如果在一台iSpirit 3524F-L3/3524G-L3**交换机上需要配置三个如下所示的**vlan:
vlan 2**的子网接口为** 172.16.3.1 **子网掩码:**255.255.255.0
vlan 3**的子网接口为**192.168.1.1 **子网掩码:**255.255.255.0
vlan 4**的子网接口为**172.16.4.1 **子网掩码:**255.255.255.0

首先需要在交换机上配置三个vlan **:**vlan2 vlan 3 vlan 4

```
Switch# vlan 2
 Vlan 2 added
Switch(vlan-2)#exit
Switch# vlan 3
 Vlan 3 added
Switch(vlan-3)#exit
Switch# vlan 4
 Vlan 4 added
```

查看vlan**的配置信息**

```
Switch# show vlan
_______________________________________________
|VID |Name                    | Status |
|----+-----------------------------+--------|
|1   |Default VLAN 1            | Static |
|-------------------------------------------|
|2   |vlan2                  | Static |
|-------------------------------------------|
|3   |vlan3                  | Static |
|-------------------------------------------|
|4   |vlan4                  | Static |
|-------------------------------------------|
```

然后在以上的基础上根据实际情况的需求参照前面的章节在每个vlan内添加交换机的端口。

然后依下面的步骤配置交换机的子网：

Switch(route-config)# ip sub
Netware Interface: 2
Agent Ip Addr: 172.16.3.1
Net Mask: 255.255.255.0
Vlan ID: 2
Interface Descript: vlan2
Switch(route-config)# ip sub
Netware Interface: 3
Agent Ip Addr: 192.168.1.1
Net Mask: 255.255.255.0
Vlan ID: 3
Interface Descript: vlan3
Switch(route-config)# ip sub
Netware Interface: 4
Agent Ip Addr: 172.16.4.1
Net Mask: 255.255.255.0
Vlan ID: 4
Interface Descript: vlan4

查看配置子网的结果

Switch(route-config)# show ip sub ta

ifIndex IP Address NetMask Vid Status Desc
01100002 172.16.3.1 255.255.255.0 2 Active vlan2
01100001 192.168.0.1 255.255.255.0 1 Active Default IP Addr
01100003 192.168.1.1 255.255.255.0 3 Active vlan3
01100004 172.16.4.1 255.255.255.0 4 Active vlan4

3.2.19.3子网的配置命令列表

在iSpirit 3524G/F-L3交换机的子网的配置功能中含有如表3-22所示的命令，

表3-22

符号	描述
ip subnet	给指定的子网和vlan添加一个网络接口地址
no ip subnet <ipaddr>	删除交换机一个子网接口
show ip subnet information	显示交换机子网接口信息

3.2.20 DHCP 中继

如果DHCP服务与DHCP客户位于不同的网段，那么网络中就必须具备有DHCP中继(即DHCP Relay)功能的IP设备，把DHCP的信息从一个网段传送到另一个网段。iSpirit 3524G/F-L3交换机具有DHCP中继的功能，启动该功能后，只要在交换机中设定DHCP服务器的IP地址就可以了。

3.2.20.1 DHCP中继的配置和管理

DHCP中继的配置和管理包含使能和关闭dhcp relay

- 打开dhcp relay 功能
  Switch#enable dhcprelay

- 关闭dhcp relay 功能
  Switch#disable dhcprelay

3.2.20.2 DHCP中继的配置实例

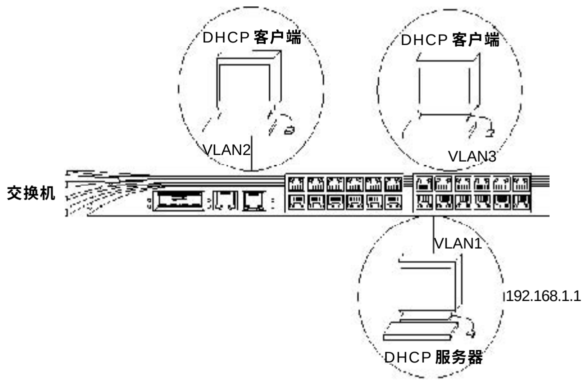


图3-17　表示DHCP中继

如图所示需要在交换机上划分有3个vlan，vlan 1作为服务器vlan ,子网IP为192。168.1.0网段，VLAN2子网的IP网段为192.168.2.0，VLAN3子网的IP网段为192。168.3.0，在VLAN1内有一台DHCP服务器，IP地址为192.168.1.1，为其他VLAN的DHCP 客户端提供IP地址分配。VLAN2和VLAN3都是用户的使用VLAN，里面的客户端都使用自动获取ip地址。

首先要确保在35交换机上配置好了vlan和子网，子网之间能够正确进行路由

然后在35交换机上执行：

命令	功能
Switch# dhcp server 192.168.1.1	给交换机指定dhcp服务器的IP地址
Switch# enable dhcprelay	打开dhcprelay 的功能

3.2.20.3 在配置dhcp过程中常见问题分析及解决

1 、确保dhcp服务器能正常工作，并且上面已经配置了几个不同子网的IP地址池

2 、dhcp服务器在其中的一个vlan内，并且和交换机之间的IP能正常通信

3 、在交换机上正确配置了dhcp server的IP地址

通过命令查看dhcp server的IP地址是否正确配置

Switch# show dhcpserver

Server Ip Address : 192.168.1.1

4 、是否打开了dhcprelay 的功能

通过在交换机上的命令查看dhcp relay 功能是否打开：

Switch# show switch

Ip Address : 192.168.0.1
Subnet Mask : 255.255.255.0
Default Gateway : 0.0.0.0
MAC Address : 00:09:ca:01:75:02
BOOTP : Disable
DHCP : Disable
Spanning Tree : Enable
Traffic Classes : Enable
IGMP Snooping : Enable
Reset : no reset
DhcpRelay : Enable

3.2.20.4 DHCP中继的命令列表

在iSpirit 3524G/F交换机的DHCP 中继功能中含有如表3-20所示的命令，

表3-23

符号	描述
disable dhcprelay	关闭dhcp relay 功能
enable dhcprelay	打开dhcp relay 功能
dhcp server <ipaddr>	设置dhcp server的ip地址功能
show dhcpserver	显示dhcp server 的ip地址

3.2.21 静态路由

用户在路由模式下配置交换机的静态路由信息。静态路由是由用户定义的、一条可使数据包从源地址通过指定路径到达目的地址的路由。当动态路由协议未能创建一条到特定目的的路由时,静态路由就显得特别重要。还可以通过配置某一静态路由为缺省路由,把无法确定路由的数据包发送到默认的网关。

静态路由是由管理员手工配置而成。适用于组网结构较简单、到给定目标只有一条路径的网络中,管理员只需配置静态路由就能使交换机正常工作。静态路由于不会有路由更新而不会占用宝贵的网络带宽。

缺省路由也是一种静态路由。简单地说，缺省路由就是在没有找到任何匹配的路由项情况下,才使用的路由。即只有当无任何合适的路由时,缺省路由才被使用。在路由表中，缺省路由以到网络 0.0.0.0（掩码为 0.0.0.0）的路由形式出现。可通过命令show ip route table 来查看它是否被设置。若报文的目的地不在路由表中且路由表中也无缺省路由存在,该报文被丢弃的同时将返回源端一个ICMP 报文指出该目的地址或网络不可达信息。缺省路由在网络中是非常有用的。在一个包含上百个交换机的典型网络中,运行动态路由选择协议可能会耗费较大量的带宽资源,使用缺省路由就可节约因路由选择所占用的时间与包转发所占用的带宽资源,这样就能在一定程度上满足大量用户同时进行通信的需求。

3.2.21.1 静态路由的配置和管理

路由的配置和管理包含路由协议的使能和关闭、静态路由的添加和删除、路由表的管理。

- 启动动态路由协议
  Switch(route-config)#ip route protocol <protocol>
  说 明 ： 参数为 r i p ，启动 RI P 协议。

- 停止动态路由协议
  Switch(route-config)#no ip route protocol

- 显示交换机上的关于路由的设置的一些信息，如整体的动态路由协议、硬件支持的子网个数、当前子网个数等信息
  Switch(route-config)#show ip route informat ion

- 添加一条静态路由信息
  Switch(route-config)#ip static route
  说 明 ： 这是一个交互式命令，要求用户输入目的 ip 地址，子网掩码，网关 ip 地址，该项信息描述，是否在硬件寄存器中保存等。其中要求用

户输入的目的ip **地址与子网掩码的与等于目的**ip **地址。即目的**ip **地址为一个网络地址。网关必须与某一个现存的子网接口地址在同一个网段内。**

示例:在交换机上添加一条缺省路由,下一跳指向192.168.2.2(**下一跳可达**)

Switch(route-config)# ip static route
Dest Ip: 0.0.0.0
Net Mask: 0.0.0.0
gate way: 192.168.2.2
Static Route Name:def
Use HareWare(y/n)y
Switch(route-config)#

- **删除给定目的地址的静态路由项**
  Switch(route-config)#no ip static route <ipaddr>
  示例：在交换机上删除缺省路由
  switch(route-config)#no ip static route 0.0.0.0 0.0.0.0

- **显示交换机上的静态路由信息**
  Switch(route-config)#show ip static route table

- **显示交换机上的所有路由信息**
  Switch(route-config)#show ip route table

3.2.21.2 静态路由的配置实例

实例配置需求:如下图所示需要通过配置静态路由,使任意两台主机或交换机之间都能两两互通。

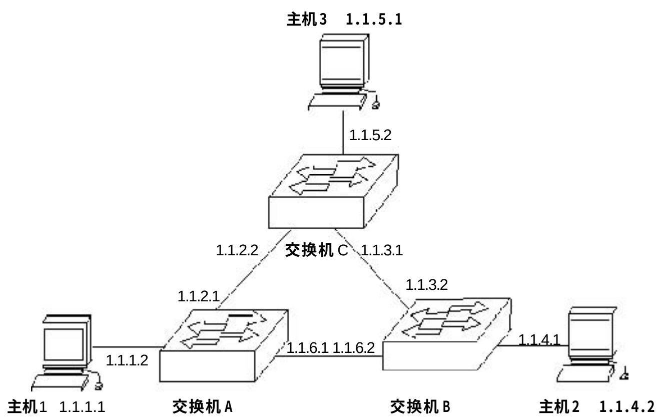


图3-18 配置静态路由的组网图

3、**具体配置**

！配置三层交换机A **的静态路由**

Switch(route-config)# ip static route
Dest Ip: 1.1.4.0
Net Mask: 255.255.255.0
gate way: 1.1.6.2
Static Route Name:a12
Use HareWare(y/n)y
Switch(route-config)# ip static route
Dest Ip: 1.1.5.0
Net Mask: 255.255.255.0
gate way: 1.1.2.2
Static Route Name:a13
Use HareWare(y/n)y

！配置三层交换机B **的静态路由**

Switch(route-config)# ip static route
Dest Ip: 1.1.5.0
Net Mask: 255.255.255.0
gate way: 1.1.3.1
Static Route Name:a23
Use HareWare(y/n)y
Switch(route-config)# ip static route
Dest Ip: 1.1.1.0
Net Mask: 255.255.255.0
gate way: 1.1.6.1
Static Route Name:a21
Use HareWare(y/n)y

！配置三层交换机C **的静态路由**

Switch(route-config)# ip static route
Dest Ip: 1.1.1.0
Net Mask: 255.255.255.0
gate way: 1.1.2.1
Static Route Name:a32
Use HareWare(y/n)y
Switch(route-config)# ip static route
Dest Ip: 1.1.4.0

Net Mask: 255.255.255.0
gate way: 1.1.3.2
Static Route Name:a31
Use HareWare(y/n)y

3.2.21.3 静态路由的配置常见问题分析解决

故障之一：接口的物理状态和链路层协议状态均已处于UP，但IP报文不能正常转发。

故障排除：

- **用**show ip static route table**命令查看是否正确配置相应静态路由。**
- **用**show ip route table**命令查看该静态路由是否已经生效。**
- **查看是否在接口上未指定下一跳地址或下一跳地址不正确。**
- **查看是否能够连通下一跳。**
- **查看指定的发送数据包的主机的指定网关是否正确。**

3.2.20.4 静态路由配置命令列表

在iSpirit 3524G/F**交换机的路由功能中含有以下命令，如表**3-24

表3-24

符号	描述
route	进入路由配置模式
ip route protocol <protocol>	启动动态路由协议
no ip route protocol	停止动态路由协议
ip static route	添加一条静态路由信息
no ip static route <ipaddr>	删除给定目的地址的静态路由项
show ip static route table	显示交换机上的静态路由信息
show ip route table	显示交换机上的所有路由表信息
show ip route information	显示交换机上的关于路由设置的一些信息

3.2.22 ACL功能

访问控制列表是应用到交换机接口的指令列表,这些指令列表用来告诉交换机哪些数据包可以接收,哪些数据包需要拒绝。至于数据包是被接收还是拒绝,可以由类似于源地址、目的地址、端口号等特定指示条件来决定。

ACL 可以设置访问控制规则和带宽限制。访问控制列表可以基于三种规则来实现：基于 IP 地址的访问控制列表、基于 VLAN 的访问控制列表、基于 PORT 的访问控制列表。

3.2.22.1 ACL功能的配置和管理

ACL功能的配置和管理包含ACL的使能关闭以及如何设置删除相关的访问控制

- **启动 ACL 为 enable 状态**
  Switch#acl
  说明：在 enable **状态时规则列表才会生效，**ACL **缺省是** enable。

- **关闭 ACL 功能**
  Switch#no acl

- **显示ACL的状态和规则列表**
  Switch#show access-list [{group-id | port | vlan}] [{port-num | vlan-id}]
  示例:
  show access-list port 5
  show access-list vlan 8

- **删除ACL的规则列表中的某一条规则**
  Switch#no access-list <{group-id | port | vlan}> <{port-num | vlan-id}>
  示例:
  no access-list vlan 20
  说明:group-id，port，vlan **是可选参数，命令行参数有以下几种情况：如果不输入其他参数，则显示** ACL **的状态和所有的规则列，如：**show accesslist**；如果输入** group-id**（即某一条规则已知的组号），则会显示这一条规则，如：**show access-list 4**；如果只输入** port **参数，会显示所有和** port **相关的规则；如果还输入了交换机端口号，只会显示和这个端口相关的信息。**group-id，port，vlan **是必选参数，命令行参数有以下几种情况：**

1 、如果输入 group-id(即某一条规则已知的组号)，则会删除这一条规则，如：no access-list 4 ；

2、 如果输入 port 参数和端口号，就会删除和这个端口相关的规则，如：no access-list port 6；3、vlan 参数和 port 参数相似；

- **设置访问控制规则**
  Switch#access-list

说 明 ：access-list 可以设置访问控制规则和带宽限制。具体如下所述

1 、基于 ip 的规则

基于 ip 的访问控制规则又有标准 ip 和扩展 ip 的访问控制规则。基于标准 ip 的访问控制规则：可以允许（permit）或拒绝（deny）转发来自一个 ip，一个网段或任意 ip 的数据包。

基于标准 ip 的访问控制规则的 group id 的范围在 1 － 99 之间。本系统一个 group id 只对应一条规则。

2 、扩展 ip 的访问控制规可以控制所有 tcp/ip 协议的数据报转发

它兼容了基于标准 ip 的访问控制规则，相对于基于标准 ip 的访问控制规则要更细化一些。如对 icmp，osp f 以及 tc p，u dp 之上的服务端口的控制: 同时提供了常用协议名称（icmp ），常用服务端口名称（www）和对应数字的输入方式。如在输入 tcp 和 6 是一样的。ip 地址可以是源 ip 或目的 ip。基于扩展 ip 的访问控制规则的 groupid 的范围在 100 － 199 之间.

3 、基于 mac 的规则

基于 mac 的访问控制规则可以允许（permit）或拒绝（deny）转发来自一个 mac 的数据包，也可以控制 mac 桢之上的协议包如 arp 包等。基于 mac 的访问控制规则的 group id 的范围在 700 － 799 之间。在基于 mac 和基于 ip 的访问控制规则中，当有两条以上的规则发生冲突时，group id 高的先有效；如：

switch# access-list 1 deny 10.0.0.1 0.0.0.255；

switch# access-list 2 permit 10.0.0.4。

第二条规则先生效。mac 地址和 ip 地址以及后面的 vlan 都是按字节匹配。如 ：

switch# access-list 3 permit 10.0.0.3，

意味着 10.0.0.1 和 10.0.0.2 都允许转发。因为 3 的二进制是 0b11，1 的二进制是 0b01，2 的二进制是 0b10。Mac 和 vlan 也是一样。

4 、基于 vlan 的规则可以允许（permit）或拒绝（deny）转发一个 vlan 的数据包。

5 、port 相关的访问控制规则

上述的基于 ip、mac、vlan 的访问控制规则都是基于交换机的。如果要让上述的规则只对某一个端口生效，就要把这个端口加入到这条规则中去。基于端口的访问控制规则只有一条规则就是 all，拒绝或允许转发所有上行或下行的数据包，主要功能是对访问带宽的控制。如果要实现基于 ip 、mac 、vl an 的访问控制则要先设置好这些基于交换机的规则，然后把相应端口加入这些规则就可以了，加入以后这个端口就属于某一条规则，如：switch# access-list 1 deny 10.0.0.1 0.0.0.255；命令switch# access-list port 4 1，把端口 4 加入到规则 1。命令 switch# access-list port 3 all in permit 4，对端口 3 进行流量控制。从上述的例子可以看到，端口可以有单独的规则，也可以加入到某一条规则中去。

6 、流量控制：本系统对以上所有的规则都可以进行流量控制

流量控制的范围是 1-20 Mb，所有要进行控制的规则都必须已经存在。命令 switch# access-list rate-limit 4 3，对 groupid 为 4 的规则带宽限制是 3 M b 。

示例: 只允许转发来自10.1.1.0/24和10.1.2.0/24两个网段之间的数据包

switch#access-list 1 permit 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255

3.2.22.2 ACL功能的配置实例

一、配置基于 IP 规则的 ACL 功能

一个交换机连接三个子网，设计ACL**，阻塞源地址为**192.168.1.0**网络地址而允许其他网络地址的通信流量通过。**

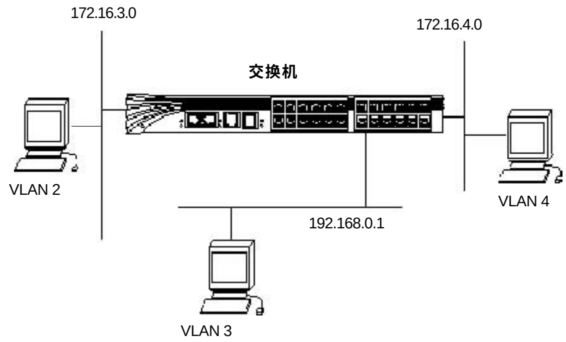


图3-19　配置基于IP 规则的ACL 功能

按照以上需求需要在交换机上做如下配置：

Switch# access 1 deny 192.168.1.0 0.0.0.255

二 、　扩展 IP 规则的 acl

在下图示的网络中，用户都在172.16.3.0**网段，数据库服务器在**172.16.4.0**网段，**ip**地址为**172.16.4.1。**为了保护服务器的安全，不允许其他网段的用户对服务器进行**ping**和**web**服务，而允许其他的服务通过。**

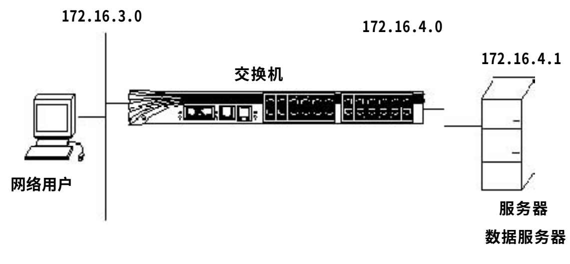


图3-20　扩展IP 规则的acl 配置

对于以上的需求需要在交换机上执行

Switch# access-list 100 deny icmp any host 172.16.4.1

Switch# access-list 101 deny tcp any host 172.16.4.1

三 、 MAC地址规则的访问控制列表

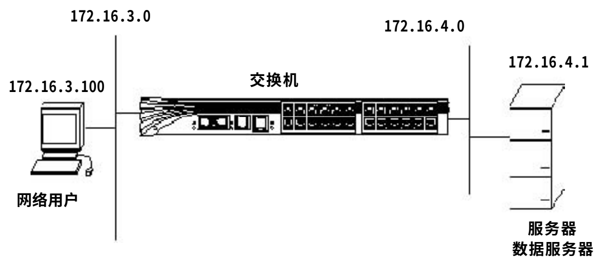


图3-21 MAC地址规则的访问

基于安全的考虑,用户有时需控制特定的mac**地址为**00:04:e2:7f:36:cf **的数据流不能通过交换机进行转发则需要在交换机上执行以下命令:**

Switch# access-list 700 deny ip 00:04:e2:7f:36:cf

四、基于 vlan 规则的 acl 功能

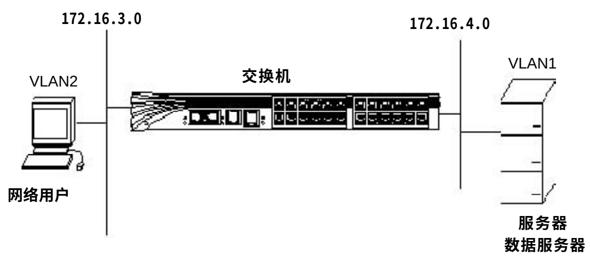


图3-22 基于vlan 规则的acl配置

当用户需要禁止转发VLAN3**的所有用户数据时可采用以下配置过程:**

Switch# access-list vlan 3 deny

排 错 :

Switch# show access-list
ACL Status : Enable

Vlan list:
VlanId 3 deny Active

五、基于 acl 规则的带宽限制功能

A: 对一个特定的端口1**的流入数据流量做**1M**带宽的限制。**

Switch# access-list port 1 all in permit 1

Switch# show access-list

ACL Status : Enable

Port list:

Port 1 permit ingress 1*125kByte/s Active

B:**基于特定访问控制列表的带宽限制**

限制源地址为192.168.1.0**网段的机器以最高**10M**的流量通过交换机**

先建立一个标准访问控制列表，以允许192.168.1.0**网段的设备流量通过交换机**

Switch# access-list 1 permit 192.168.1.0

然后对这条访问控制列表进行10M**的带宽控制，**

Switch# access-list rate-limit 1 10

通过show**命令进行带宽配置查看**

Switch# show access-list 1

ACL Status : Enable

Standard IP access list:

GroupId 1 permit srcIp 192.168.1.0 any 10*125kByte/s Active

六、基于 port 的 acl 规则

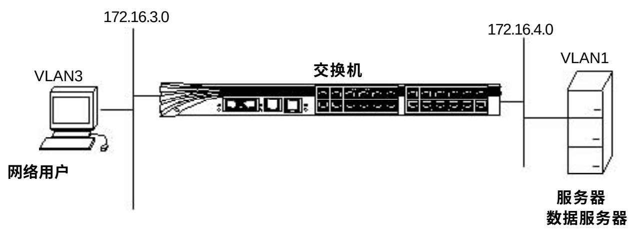


图3-23 基于port的acl规则

默认情况下访问控制列表是应用于整个交换机上的需要将访问控制列表加载到特定的交换机端口，仅仅对接入此端口的用户起作用。例如，一网络用户连接到此交换机上的端口6**，需要在此端口上添加一条访问控制列表用于阻止**172.16.3.100**用户访问通过此交换机访问网络。对以上需求需要进行以下配置：**

1 **、先建立一条访问控制列表（默认是应用于整个交换机的）**

Switch# access-list 1 deny host 172.16.1.100

2 **、应用此访问控制列表于**35**交换机端口**6

3.2.22.3 ACL功能的配置常见问题分析解决

配置基于 IP 规则的 ACL 功能常见问题分析及解决

在配置访问控制列表之前确定所有ip**之间都是通的，然后再添加访问控制列表**

这条访问控制列表阻塞的是源地址为192.168.1.0**网段的**IP**数据流通过交换机。注意子网反码的写法。用**show access-list **命令列出访问控制列表进行查看，一定要注意源地址和目的地址不要写反。然后进行访问控制列表的查看。**

Switch# show access-list

ACL Status : Enable

Standard IP access list:

GroupId 1 deny srcIp 192.168.1.0 0.0.0.255 any Active

配置扩展 IP 规则的 acl 功能常见问题分析及解决

在配置访问控制列表之前确定所有 ip 之间都是通的，然后再添加访问控制列表

对于特定的应用需要指定特定四层网络端口

还需要用show access-list **命令来进行查看访问控制列表配置是否正确**

用show access-list **命令进行查看**

Switch# show access-list

ACL Status : Enable

Extended IP access list:

GroupId 100 deny icmp any destIp 172.16.4.1 Active

GroupId 101 deny tcp any 0 destIp 172.16.4.1 www Active

配置 MAC 地址规则常见问题分析及解决

用户用以下命令来确定访问控制列表的配置正确性

Switch# show access-list

ACL Status : Enable

MAC address list:

GroupId 700 deny ip srcMac 00:04:e2:7f:36:cf Active

基于 port 的 acl 规则常见问题分析及解决

Switch# show access-list

ACL Status : Enable

Standard IP access list:

3.2.22.4 ACL功能命令列表

在 iSpirit 3524G/F 交换机的 ACL 功能中含有以下命令，如表3-25

表3-25

符号	描述
acl	启动ACL为enable状态
no acl	关闭ACL功能
show access-list [{group-id | port | vlan}] [{port-num | vlan-id}]	显示ACL的状态和规则列表
no access-list <{group-id | port | vlan}> <{port-num | vlan-id}>	删除ACL的规则列表中的某一条规则
access-list	设置访问控制规则

3.2.23 RIP 协议

RIP 是 Routing Information Protocol （即路由信息协议）的简称,是 Internet 中常用的路由协议。它是一种内部路由协议。RIP采用距离向量算法,即路由器根据距离选择路由，所以也称为距离向量协议。RIP是一种基于V-D 算法的协议，它通过UDP（User Datagram Protocol）数据报交换路由信息，每隔 30 秒向外发送一次路由更新。如果路由器经过180秒没有收到来自对端的路由更新信息,则将所有来自此路由器的路由信息标志为不可达,并且如果在其后60秒内仍没有收到更新信息就将其删除。RIP 运行简单，适用于小型网络.

RIP 使用跳数（hop count）来衡量到达信宿机的距离，称为路由权（Routing Metric）。在 RIP 中路由器到与它直接相连的网络的跳数为 0（在某些协议中被定义为 1），到通过一个路由器可达的网络的距离为 1 跳，其余依此类推。为限制收敛时间，RIP 规定 metric 为 1~15 间的整数，若跳数超过或等于 16 位被当作无穷大。

RIP 有 RIP-1 和 RIP-2 两个版本，RIP-2 支持明文认证和 MD5 密文认证，并支持可变长子网掩码。

RIP 启动和运行的整个过程可描述如下：

(1) 某路由器刚启动 RIP 时，以广播形式向其相邻路由器发送请求报文，相邻路由器收到请求报文后，响应该请求，并回送包含本地路由信息的响应。

(2) 路由器收到响应报文后，修改本地路由表，同时向相邻路由器发送触发修改报文，广播路由修改信息。相邻路由器收到触发修改报文后，又向其各自的相邻路由器发送触发修改报文。在一连串的触发修改广播后，各路由器都能得到并保持最新的路由信息。

(3) 同时，RIP 每隔 30 秒向其相邻路由器广播本地路由表，相邻路由器在收到报文后，对本地路由进行维护，选择一条最佳路由，再向其各自相邻网络广播修改信息，使更新的路由最终能达到全局有效。同时，RIP采用超时机制对过时的路由进行超时处理，以保证路由的实时性和有效性。RIP 作为 IGP 协议的一种，正是通过这些机制，使路由器能够了解到整个网络的路由信息。

例：下图所示为 RIP 协议的运行过程。

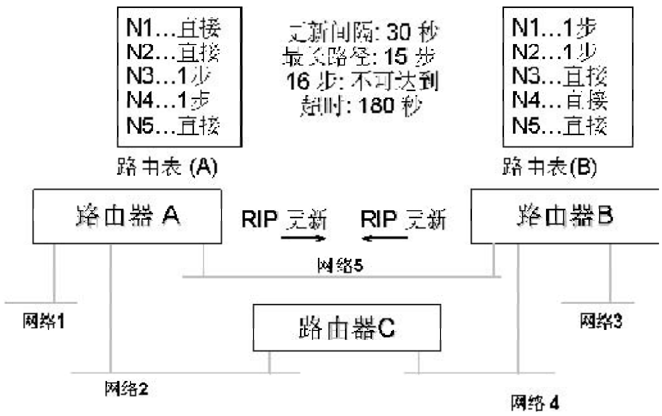


图 3-24 RIP协议工作过程

在网络 5: 路由器 A 每隔30秒钟向自己的邻居广播自己的路由表.

在网络 5: 路由器 B 每隔30秒钟向自己的邻居广播自己的路由表.

路由器 A 和 B 更新自己的路由表.

路由器不能有超过15的步长值. 如果步长为16则认为网络是不可到达的.

如果路由器有 6 次(缺省 = 180 秒) 不能收到期望的路由器更新，则当它自己广播时,就会宣布前面收到的路由是非法的.

虽然 RIP 目前已被大多数路由器厂商所广泛使用，但它还是有较大的局限性：

- 支持站点的数量有限：这就使得 RIP 只适用于较小的自治系统，如只用于大多数校园网及结构较简单的连续性强的地区性网络。
- 依靠固定度量计算路由：RIP 不能实时更新度量值来适应网络发生的变化，在人为更新之前，由网络管理员定义的度量值仍是固定不变的。

路由表更新信息将占用较大的网络带宽：RIP 每30 秒就向外广播发送路由更新信息。在有许多节点的网络中，这样将消耗相当大的网络带宽。

3.2.23.1 RIP协议的配置和管理

RIP 协议的配置和管理包含 rip 路由的基本配置的设置、静态路由的重分发、以及察看等相关的指令。3524G/F-L3 交换机默认的 rip 是关闭的。

- 显示 rip 协议配置信息，带参数是显示指定接口的配置信息，不带参数是显示所有接口的配置信息
  Switch(rip_config)#show rip [<ipaddr>]

- 配置 rip 协议的认证 type，这是一个交互式命令，首先要求输入接口 ipaddr，
  然后是 authentication type，可以是“text“，“md5”两种形式。(现 md5 不可用)
  Switch(rip_config)#auth type

- 配置 rip 协议的 send type, 这是一个交互式命令，首先要求输入接口 ipaddr；然后是 send type，可以为“nosend”，“v1”，“v2”，“v1 compatible”，“v1demand”，“v2demand”
  Switch(rip_config)#send type

- 配置 rip 协议的 receive type，这是一个交互式命令，首先要求输入接口 ipaddr；然后是 rece ive ty pe, 可以为“v1”，“v2”，“v1|v2”，“norecei”。
  Switch(rip_config)#receive type

- 配置 rip 协议的标准为默认标准, 这是一个交互式命令，首先要求输入接口 ipaddr， 然后是 default met ric，距离大小是 0-15
  Switch(rip_config)#default metric

- 更新 RIP 协议使用的三个时钟计时器：路由更新计时器、路由超时计时器、路由清空计时器。
  Switch(route-config)# timers
  说明:路由更新计时器缺省为 30 秒，路由超时计时器缺省为 180 秒，路由清空计时器缺省为 300 秒。该命令是一个交互式命令。首先输入 update timer,接着输入timeout timer,最后输入garbage timer,若用户不输入相应值，直接按回车，则保持该值不变。

- **将静态路由信息重新分发到**rip **协议**
  Switch(rip_config)#redistribute
  示例:
  Switch(rip_config)# red
  Protocol Name(static):static
  Default Metric(0-15):2
  static is transferred now

- **关闭**redistribution **功能，用户可选择是否保存原有路由**
  Switch(rip_config)#no redistribute
  说明: 关闭redistribution **功能，用户可选择是否保存原有路由**
  示例:
  Switch(rip_config)# no red
  Protocol Name(static):static
  Keep old routes(Yes/No):yes
  only static is supported now

- **端口收发各种报文的统计功能**
  Switch(rip_config)#showstats

3.2.23.2 RIP协议的配置实例

如下图所示三台交换机两两相连，分别有6**个网段，都启用**rip**协议，实现三台**PC**机之间能够两两互通。**

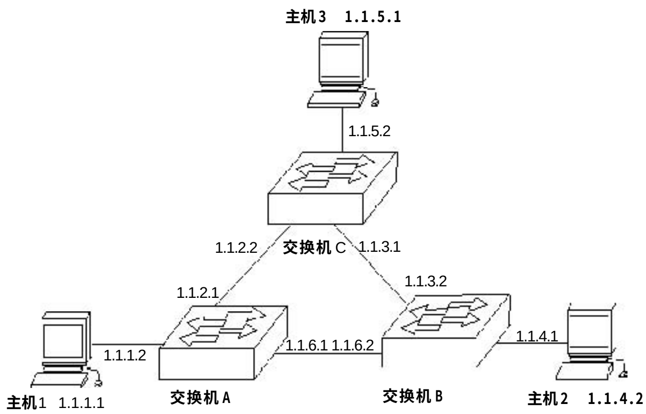


图3-25 RIP协议的配置实例

配置步骤：

在每台交换上配置Switch (route_config)# ip route protocol rip

图 3-27 的组网需求：三层交换机 A 与 B， A 与 C 分别相连，若交换机 A（192.1.1.1）只想把路由更新信息发送到相邻交换机 B （ 192.1.1.2）而不发给相邻路由器 C。

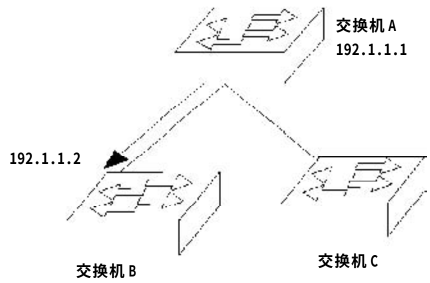


图3-26 RIP协议的组网图

根据图3-26的组网需求需要进行以下的配置步骤

(1) **进入交换机A的路由模式**

(2)**设置交换机 A 某一接口的发送类型为“** nosend”

Switch(rip_config)# send type

Interface Ip address:192.1.1.1

Send Type:nosend

表 3-23 含有 iSpirit 3524G/F 交换机的 RIP 协议功能命令。

表3-23

符号	描述
rip	进入rip配置模式
ip route protocol rip	启动rip协议
show rip [<ipaddr>]	显示rip协议配置信息
auth type	配置rip协议的认证type
auth key	配置rip协议的认证key
send type	配置rip协议的send type
receive type	配置rip协议的receive type
timers	更新rip协议使用的三个时钟计时器
default metric	配置rip协议的标准为默认标准
redistribute static	将静态路由信息引入到rip协议
split horizon	启动rip协议的水平分割功能，减少路由环路的出现的可能性
no splithorizon	取消rip协议的水平分割功能。
no redistribute	从rip协议中取消静态路由的信息

第4章
菜单界面配置

本章主要说明iSpirit 3524G-L3/iSpirit 3524F-L3**交换机以下内容**:

1、**菜单界面综述**
2、**菜单界面详细介绍**

4.1 菜单界面综述

4.1.1 菜单界面的特点

联想天工iSpirit 3524G-L3/iSpirit3524F-L3**交换机使用嵌入式**ANSI/VT100**菜单界面管理配置交换机。其主要特点是：**

- **具有方便快捷的管理和配置机制。**
- **方便启用**telnet**访问交换机**
- **避免通过** Web **访问时图形对象显示带来的时延。**

下面以3524G-L3**为例对菜单界面进行说明。**

4.1.2 菜单界面的应用说明

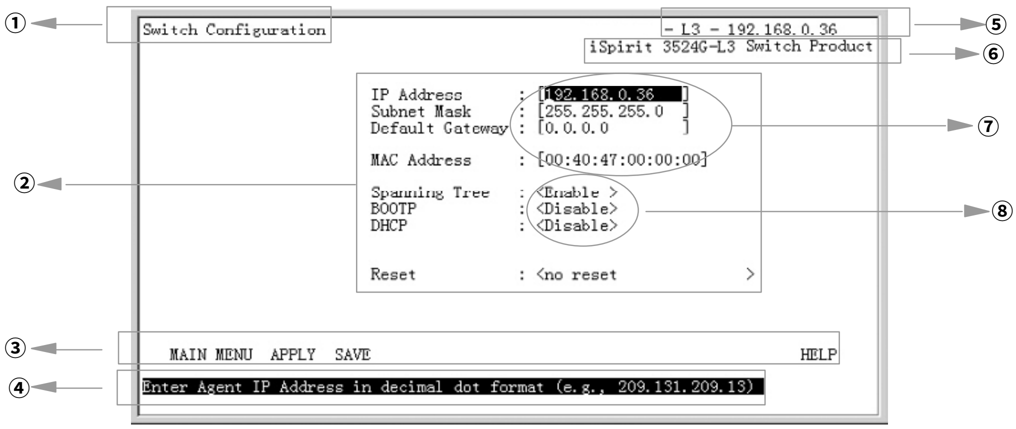


图4-1 菜单界面示图

如图 4-1 所示，菜单界面包括以下几个部分：

①显示当前页的题目
② 显示正文内容，用户可以在此键入文本或切换域值
③ 显示命令栏，该命令栏是一个横向的菜单
④显示帮助信息
⑤ 显示交换机的IP地址
⑥显示交换机的型号及版本

主要使用的域类型如表 4-1 所示。

表4-1

域类型	说明	图例
显示域	显示域显示只读信息	见图4-1标注①④⑤⑥
编辑域	文本编辑域括在中括号〔〕里，可被用户输入编辑。当前文本编辑域以反白方式显示	见图4-1标注⑦
切换域	切换域括在角括号<>里，允许用户从一列预定义的值中选择一值。 按空白键进行值切换，当前文本编辑域以反白方式显示	见图4-1标注⑧
菜单域	使用TAB或箭头键（只有在Telnet方式中可用),选择一菜单项，然后按回车确认	见图4-1标注③

一般命令栏项的作用见表 4-2。

表4-2

键	作用
MAIN MENU	返回主菜单
APPLY	将交换机或管理主体界面上的值放到内存中。
SAVE	做APPLY的工作，然后在非易失性存储器中存储所有配置变量值。因为存储操作需要擦写Flash芯片，这要占用一定时间，所以建议用户在做完所有改动之后，再按Save按钮。

菜单界面使用的导航键的作用见表4-3（注意：忽略ESC键，被选域以反白方式显示）。

表4-3

键	作用
TAB	向右、向下经过菜单项和编辑域（与→和↓键作用相同）
ENTER	经过菜单项点击该键，相应项被选择，其他功能与TAB键相同
→	向右、向下经过菜单项和编辑域（与TAB和↓键作用相同）
←	向左、向上经过菜单项和编辑域（与↑键作用相同）
↓	向右、向下经过菜单项和编辑域（与TAB和→键作用相同）
↑	向左、向上经过菜单项和编辑域（与←键作用相同

注意：→、←、↓、↑只在Telnet方式下有效。

在文本编辑域中菜单界面使用的键及键的作用见表4-4(注意:在编辑文本时忽略ESC和箭头键)。

表4-4

键	作用
Alpha/numeric	当第一个字符输入时替换原来的域文本，alpha/numeric键是包含标点在内的可显示的ASCII键，但不包括TAB键。
BACKSPACE	删除前一个字符（与DELETE键同）
DELETE	删除前一个字符（与BACSPACE键同）
ENTER	如果域值正确，则接受域值并转移到下一域。如果域值不正确（如无效的IP地址格式），重储该域原值，光标停留在当前域。
ESC	取消对域值的改变，显示原值，光标停留在当前域。

在切换域中菜单界面使用的键及键的作用见表4-5（注意：在切换域值时忽略ESC)。在表4-5端口统计信息界面，端口域不遵循以上切换域规则。对于该域，当前显示值马上被使用。

表4-5：

键	作用
↓	接受切换域值，转移至下一域（与→作用同）
ENTER	接受切换域值，转移至下一域（与TAB作用同）
←	接受切换域值，转移至上一域（与↑作用同）
→	接受切换域值，转移至下一域（与↓作用同）
SPACE	在可选项间进行切换
TAB	接受切换域值，转移至下一域（与ENTER作用同）
↑	接受切换域值，转移至上一域（与←作用同）

4.2 菜单界面详细介绍

4.2.1 菜单界面的开启

用户在 CLI CONFIGURATION 模式下，Menu 命令进入，如图 4-2 所示。用户可以通过终端模拟软件或 telnet 应用软件显示该界面。

通过 telnet 开启菜单界面前用户需要确认以下两点之一：

❶ 用户计算机已通过console控制端口对交换机设置了与用户网络一致的IP地址及子网掩码。

❷ 用户计算机与交换机建立 telnet连接。

4.2.2 主菜单界面

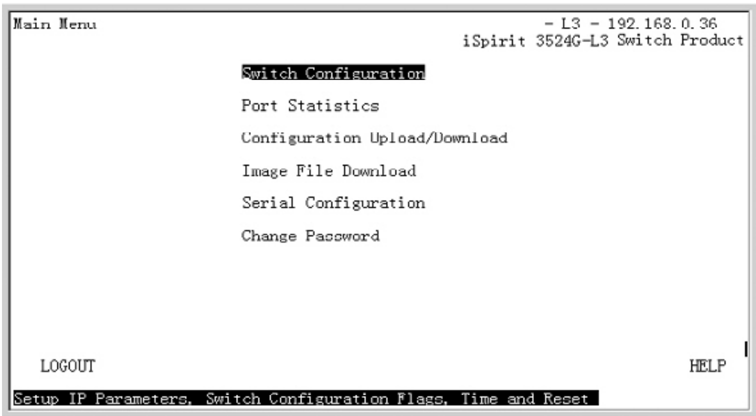


图4-2 主菜单界面

图 4-2 显示主菜单界面。当一个菜单项被突出显示，按下回车键可以进入子菜单界面。如果用户点击“*LOGOUT*”，将回到 CLI 界面方式。

4.2.3 交换机配置界面

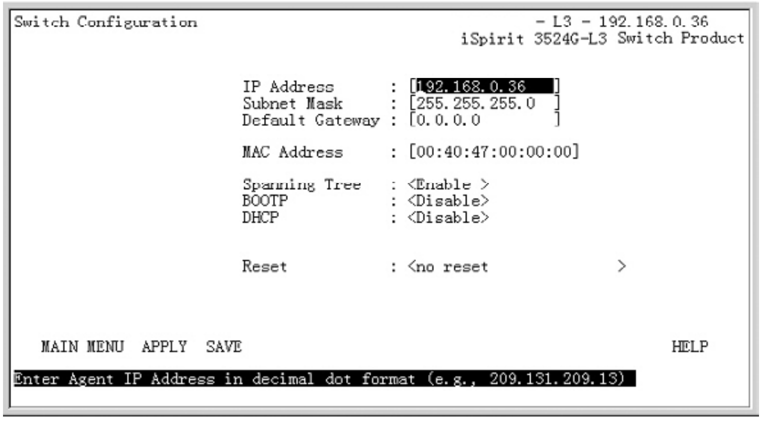


图4-3 交换机配置界面

图4-3显示交换机配置界面。用户需要在IP地址域、子网掩码域和默认网关域分别输入十进制点分格式IP地址、子网掩码和默认网关，在MAC地址域输入十六进制的MAC地址。在应用(APPLY)过程中，如果reset域选择了reset或reset factory defaults，将显示图4-4所示的重启交换机警告页面。

该界面域切换信息如表4-6所示。

表4-6

域	切换值	缺省
Spanning Tree	enable, disable	enable
BOOTP	enable, disable	disable
DHCP	enable, disable	disable
Reset	no reset, reset, reset factory defaults	no reset

4.2.4 交换机警告界面

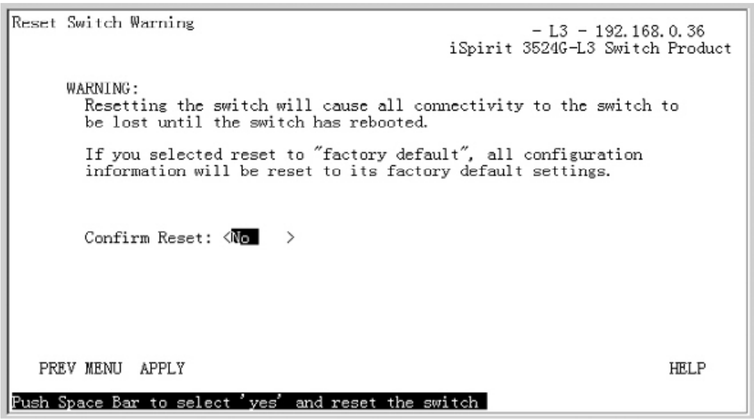


图4-4重启交换机警告页面

图4-4显示重启交换机警告页面。在应用（APPLY)过程中，如果reset域选择了reset或reset factory defaults就会显示该页面。选择yes进行重启操作，选择no取消操作。

该界面域切换信息如表4-7所示。

表4-7

域	切换值	缺省
Reset Switch	No, Yes	No

注意： 选择“reset factory”会使配置回到出厂缺省状态。

4.2.5 端口统计信息界面

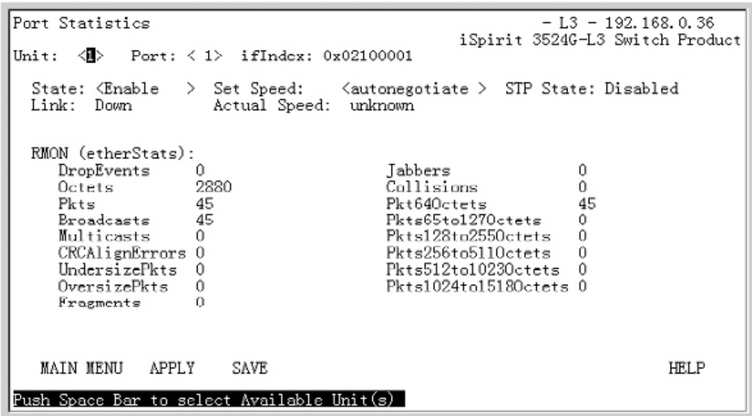


图4-5端口统计信息界面

图 4-5 显示端口统计信息界面。端口域不遵循编辑域键中切换域的规则，该域及时更新当前显示值，不用先应用（APPLY)或存储（SAVE)。使用 *State* 域启用或禁用所选端口，使用 *Set Speed* 设置端口速率。

域切换信息如表 4-8 所示。

表4-8

域	切换值	缺省
Port	1,2,...,26	1
State	enable, disable	enable
Set Speed	Autonegotiate,half-10,full-10,half-100,full-100	Autonegotiate

4.2.6 配置文件上下载界面



图4-6 配置文件上下载界面

图4-6显示配置文件上下载界面。在*Image Path*域输入配置文件的文件名。在TFTP服务器IP地址域输入TFTP服务器IP地址。方向域支持：*switch-to-host*（上载）和*host-to-switch*（下载）。

注 意 ：

1、必须在计算机上运行 TFTP server 程序。
2、设置好配置文件路径。
3、保证交换机与计算机网络连通性。

4.2.7 Image 文件下载界面



图4-7 Image文件下载界面

图 4-7 显示 Image 文件下载界面。该页面允许用户把 Boot ROM 或 Application Image 下载到 Flash ROM 中。

注意：用户必须重启交换机才能运行下载程序。

该界面域切换信息如表 4-9 所示。

表4-9

域	切换值	缺省
Download Type	Application, Boot ROM	Application

4.2.8 串口配置显示界面

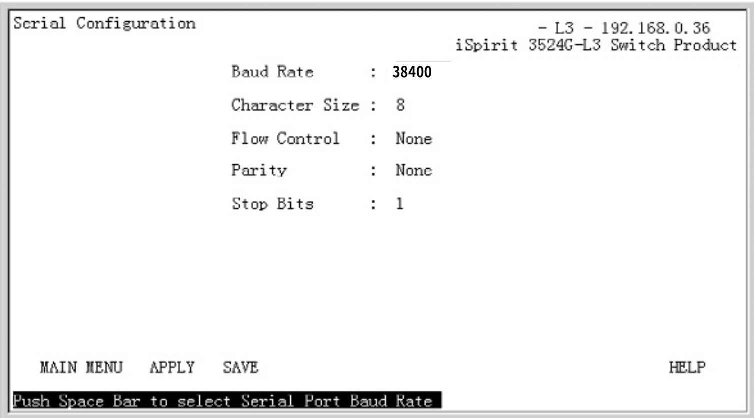


图4-8串口配置显示界面

图 4-8 **显示串口配置显示界面。该页显示只读的串口配置信息。**

4.2.9 修改密码界面

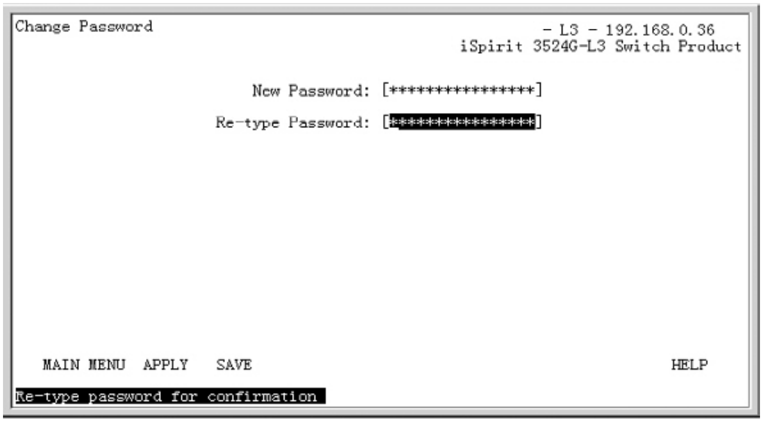


图4-9 修改密码界面

图4-9**显示修改密码界面。密码是一个最长**16**个字符区分大小写的字符串。为改变密码，用户需要先输入一遍新密码，然后再输入一遍以做确认。**

第 5 章

WEB 页面的设置

本章主要说明iSpirit 3524G-L3/iSpirit 3524F-L3**以下内容**:

1、Web **页面综述**
2、**各页面详细介绍**

5.1 Web 页面综述

5.1.1 Web 访问功能的特点

联想天工iSpirit 3524G-L3交换机为用户提供Web访问功能。用户可以通过Web浏览器访问交换机的相关信息及管理、配置交换机。其主要特点是：

- 易于访问：用户可以从网络的任何地方轻松访问交换机。
- Nestscape Communicator,Microsoft Internet Explorer等用户熟悉的浏览器都可以对联想天工iSpirit 3524G-L3交换机Web页面进行访问。
- 丰富的子页面包括：管理配置页面、通告页面、生成树页面、VLAN/ 多播组配置页面、RIP 路由基础结构页面及 RIP 页面等六大部分，其中各部分又包含各自子页。为用户提供完备的交换机管理配置途径。
- 特征信息的分类整合，便于用户查看修改信息。

5.1.2 Web 浏览的系统需求

Web 浏览的系统需求如表 5-1 所示。

表5-1

硬件与软件	系统需求
CPU	奔腾586以上
内存	32MB以上
分辨率	800x600以上
颜色	256色以上
浏览器	IE4.0以上或Netscape4.01以上
操作系统	Microsoft® ,Windows95®,Windows98®,WindowsNT®,Windows2000®,WindowsXP®,WindowsME®,Linnx,Unix类操作系统

注意： Microsoft®,Windows95®,Windows98®,WindowsNT®,Windows2000®,WindowsXP®,WindowsME®是微软公司的注册商标，所有其它产品名，商标，注册商标和服务标记，版权由各自所有者持有。

5.1.3 Web 浏览会话的登陆

在启动 Web 浏览会话前用户需要确认：

❶ 已经对交换机进行了 IP 配置，这部分内容参考第 4 章。

❷ 已将一台安装有 Web 浏览器的 PC 机或 UNIX 工作站连接到网络上。完成以上两项工作后,用户在浏览器的地址栏输入交换机的地址并按回车后即可进入交换机 Web 登录页面（如图 5-1 所示）。

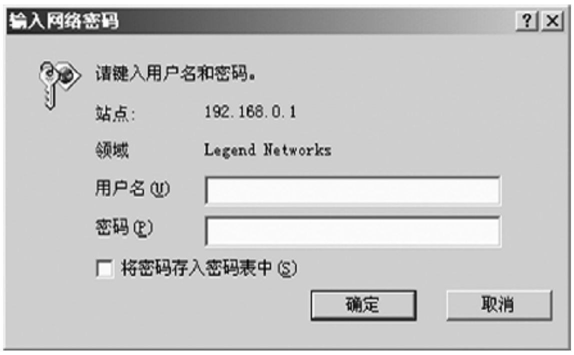


图5-1 联想天工iSpirit 3524G-L3交换机登录页面

5.1.4 Web 页面基本组成



图5-2 WEB页面基本组成

图 5-2 显示每一页面由三部分构成：lenovo 标题页、导航树页和主页面。

lenovo 标题页	用于显示 lenovo 徽标。
导航树页	用户可以打开树上的文件夹，从中选择要打开的页面。
主页面	用于显示用户从导航树中选择的页面。

5.1.5 导航树结构

图 5-3 显示导航树的组织结构。

导航树位于每一页面的左下方，用于定向用户想打开的页面。根据网页功能的不同我们将其划分成不同的组，各组又以可能被用到的频率的高低排序。大多数导航树中的网页名是相应的网页上部的网页标题的缩写。



图5-3 导航树的组织结构

5.1.6 页面选择按钮

表5-2说明页面选择按钮的作用

表5-2

按钮	作用
Refresh	更新页面上的所有域
Apply	将更新过的数值放到内存中。因为错误检查由Web服务器完成，所以在用户选择该按钮前，没有错误检查
Save	做Apply的动作，并且在非易失存储器中存储所有配置变量。因为存储操作需要擦写Flash芯片,这要占用一定时间，所以建议用户在做完所有改动之后，再按Save按钮。
Delete	删除当前记录。Next当所有条目在一页显示不下时，按下该按钮将显示下一页条目。

5.1.7 出错信息

如果服务器在处理用户请求时出现错误，就会在一个对话框中显示相应的出错信息。图 5-4 显示一个出错信息对话框。



图5-4 出错信息对话框

5.1.8 条目域

可以显示 SNMP MIB 表的网页在表的最左列有一个条目域(Entry)(如图 5-5 所示),通过该域可以访问表中的不同行。当你选择某一入口值，那一行的相应信息就显示在首行，这时只有该行可被编辑，该行又称为活动行。当最初加载一页时，入口域显示 new，活动行为空。

如果想加入新行，要从条目域的下拉菜单中选择 new，输入新行信息，然后按存储（SAVE)或应用（Apply）键。

如果想编辑已经存在的行，要从入口域的下拉菜单中选择相应的行号，根据需要编辑改行，然后按存储（SAVE)或应用（Apply）键，你会看到相应的改变在该表的只读部分显示出来。

如果想删除一行，要从入口域的下拉菜单中选择相应的行号，然后按删除（Delete）键，该行会从该表的只读部分消失。



图5-5 条目域

5.1.9 状态域

几个可以显示 SNMP MIB 表的网页在表的最右列有一个状态域（Status）（如图 5-6 所示），该域显示该行状态。由于所有行状态的改变都是在内部处理完成，所以该状态域是只读的。一旦一行中所有域都有效，该行状态就自动变成活动态 active。

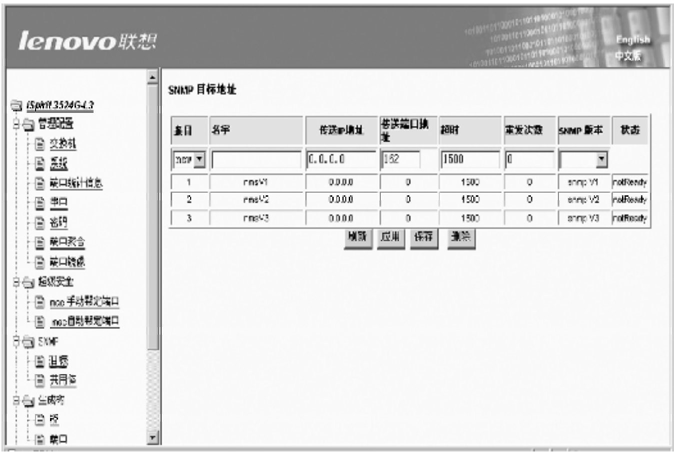


图5-6 状态域

5.2 各页面详细介绍

联想天工iSpirit 3524G-L3/3524F-L3交换机提供以下网页。下面以3524G-L3为例对各页面进行详细介绍。

页标题	说明
➲ 登录对话框	需要用户提供用户名及密码以登陆Web网页
➲ 交换机配置	设置IP地址及基本的交换机参数
➲ 系统配置	包含MIB II系统参数和产品名
➲ 端口统计信息	提供端口控制（如：enable/disable，speed/duplex 等）
➲ 串口	显示串口波特率及其它有关串口的信息
➲ 更改用户密码	更新用户密码，新的用户密码必须输入两次
➲ 端口聚合	用户可以将多个端口聚集成一组以有效的集合带宽。
➲ 端口镜像	允许用户配置端口镜像
➲MAC手动帮定端口	手动帮定端口的MAC地址及VLAN ID
➲MAC自动帮定端口	自动帮定端口的MAC地址及VLAN ID
➲ SNMP 目标	使用SNMP-TARGET-MIB说明SNMP管理对象
➲ SNMP 共用体	配置访问代理的共用体
➲ 生成树桥(Bridge)参数设置	查看并编辑生成树桥(Bridge)参数。
➲ 生成树端口参数设置	查看并编辑生成树端口参数

页标题	说明
➲ 当前 VLAN配置	显示当前 VLAN 配置（包括动态配置和静态配置）
➲ 静态 VLAN配置	通过 VID 配置静态 VLAN 配置
➲ 当前多播的分组	显示当前多播的分组(包括动态分组和静态分组)
➲ 配置静态多播	通过 VID 和 MAC 地址配置静态多播
➲IP 子网配置	显示与VLAN相关联的子网配置
➲ 静态路由配置	显示静态路由配置
➲IP 路由表页面	显示路由表信息
➲RIP 配置页面	显示现存接口对RIP协议的配置
➲RIP 统计信息页面	显示运行RIP后的统计信息
➲Radius 配置	显示认证服务器在交换机上的配置
➲802.1x协议参数配置	显示交换机上的802.1x协议配置情况
➲802.1x协议对端口的配置	显示管理员对交换机各个端口关于802.1x的配置情况
➲用户在交换机上的认证状态	显示交换机上用户的认证状态
➲ 用户信息管理	显示了用户的信息维护页面

5.2.1 登录对话框

图5-7**显示登录对话框，该登录对话框在用户第一次登录网页时显示。用户在相应的域输入用户名及密码，然后按下**OK**键就可以登录**Web **服务器。密码区分大小写，并且最多可以设置**16**个字符。厂家提供缺省密码。**

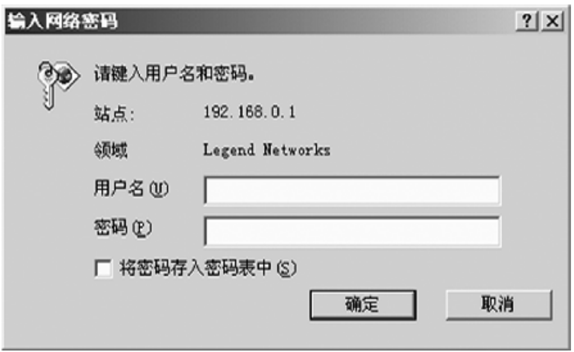


图**5-7 **登录对话框

5.2.2 主页面

图5-8**显示联想天工**iSpirit 3524G-L3**交换机主页面。该页面会在用户登录网页或点击导航树时显示出来。**

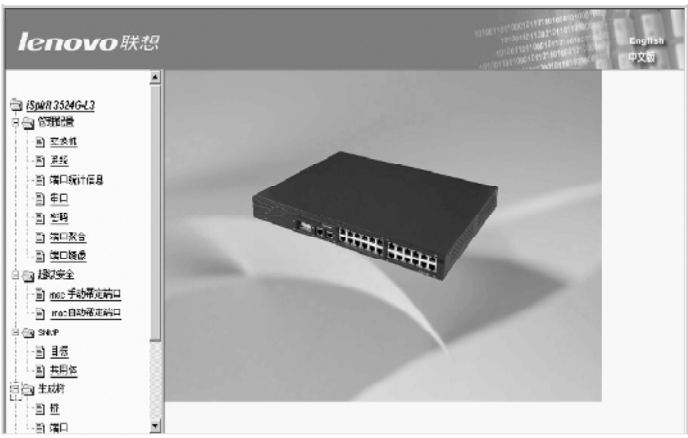


图**5-8 **联想天工**iSpirit 3524G-L3**交换机主页面

5.2.3 管理配置页面

5.2.3.1 交换机配置页面

图5-9显示交换机配置页面，该页可以让用户编辑一般性的交换机配置信息。用户以十进制格式输入IP地址、子网掩码及默认网关，以十六进制格式输入MAC地址。如果用户想重启交换机，则需要从Reset下拉菜单中选择reset或者reset factory defaults，然后按下应用（Apply）或保存（Save）键。在交换机重启前，将提示用户确认选择。

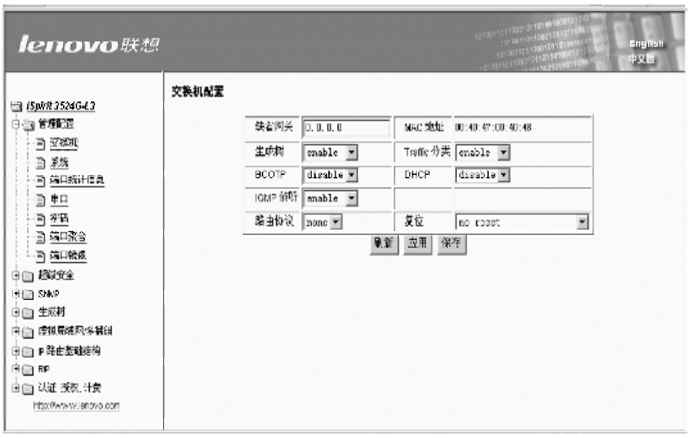


图5-9 交换机配置页面

5.2.3.2 系统配置页面

图5-10显示系统配置页面,该页面可以让用户查看并修改一些MIB II系统组对象和OEM产品。MIB产品名在控制台和Web页面上都有显示。



图5-10系统配置页面

5.2.3.3 端口配置和统计信息页面

图5-11显示端口配置和统计信息页面。该页可以让用户启用或禁用端口，设置端口速度，或显示端口的统计信息。为设置或查看某一特定端口，用户需要从 Unit 和 Port 的下拉菜单中选择相应的数字。



图5-11 端口配置和统计信息页面

页面上的下拉菜单中各项显示信息如下表所示。

表 5-3：

域	下拉菜单值	注释
Unit	1	
Port	1,2,..,26	缺省：1
State	enable，disable	缺省：enable
Set Speed(10/100Mbps ports)	autonegotiate，half-10,full-10half-100，full-100	基于端口类型(端口1到端口24)

5.2.3.4 串口配置显示页面

图 5-12 显示串口配置显示页面，该页显示串口波特率及其它有关串口的信息。

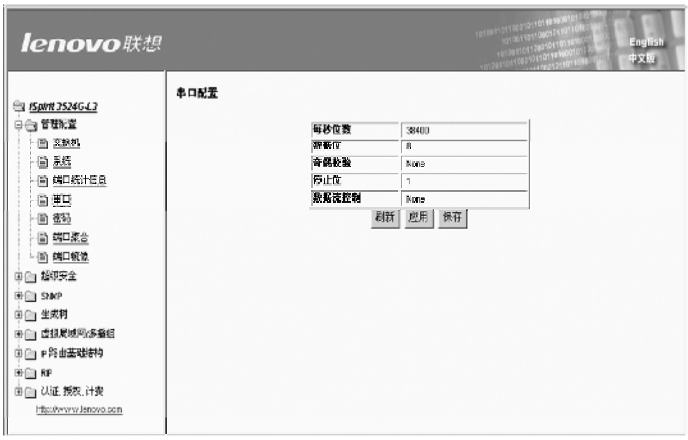


图5-12 串口配置页面

5.2.3.5 密码修改页面

图 5-13 显示密码修改页面，密码区分大小写，并且最多可以设置 16 个字符。如果要修改密码，用户需要输入新密码，并在此输入密码以做确认。一旦用户按下应用（APPLY）或存储（SAVE）键，新密码就被激活，这时会显示登录对话框（如图 5 所示）。为重新登录网页，用户必须重新输入密码并按下 OK 键。



图5-13 密码修改页面

5.2.3.6 端口聚合配置页面

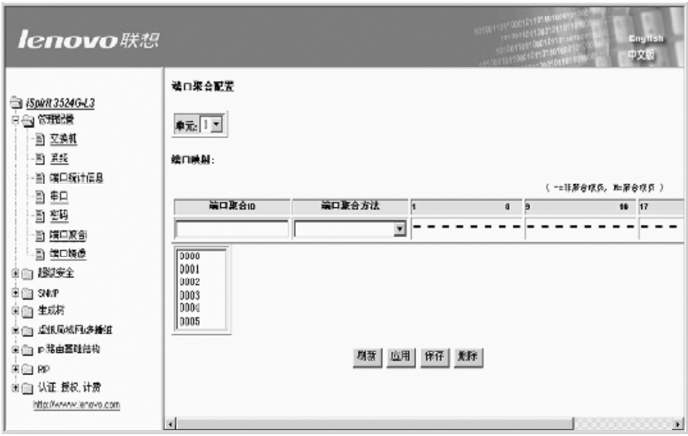


图5-14 端口聚合配置页面

图5-14显示静态端口聚合页面，该读写页面允许用户配置端口聚合。该页面由三部分构成：端口聚合组号、端口列表选择和端口聚合方法选择。

为创建或编辑端口聚合，用户需要点击列表框中相应的端口聚合组号。该端口聚合将显示在活动行中，用户可以根据需要进行编辑。当编辑结束时，按下应用（Apply）或存储（SAVE）键。

用户可以选择以6种端口聚合方式：基于源MAC地址，基于目的IP地址，基于源和目的MAC地址，基于源IP地址，基于目的IP地址，基于源和目的IP地址。

在每一个端口处点击鼠标，在表5-4列出的端口不同值间进行切换。

表5-4：

字符	全称	含义
-	Non-member	该端口不是这一端口聚合的成员
M	Member	该端口是这一端口聚合的成员

注意：支持一个端口聚合，4个10/100BaseTM端口或2个1000M端口聚合。

5.2.3.7 端口镜象页面

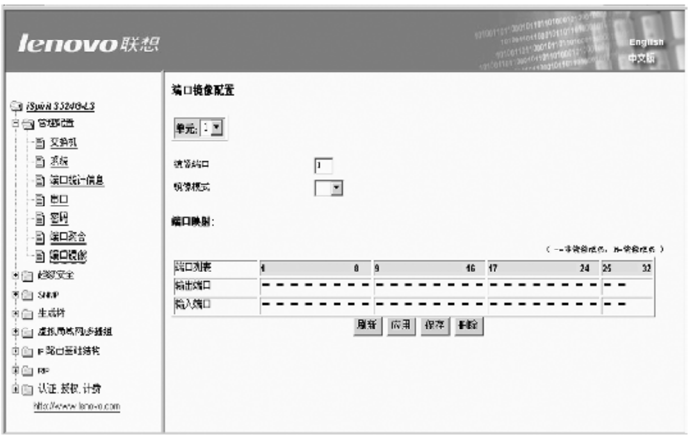


图5-15 端口镜象页面

图 5-15 显示端口镜像页面，该页面允许用户配置端口镜像，包括以下几个部分：镜像端口，镜像模式，输出端口和输入端口。

端口镜像是通过镜像端口侦听输出端口和输入端口的数据包，其取值范围是1-26。镜像模式有 l2（支持二层的数据包）和 l3（支持三层的数据包）两种，可以在下拉条中选择镜像的模式。输出端口和输入端口是被侦听的端口。

5.2.4 超级安全页面

5.2.4.1 手动绑定

手动绑定中需要用户输入 mac 地址和 vlan id，选择合适端口绑定，按下绑定按钮后，显示在绑定页面下面，同时输入信息清零。显示表中每一行前方有一小方框，便于用户删除。当用户选择若干个不需要的项后，选择解绑定按钮，将一次删掉用户所选的表项，也可选择全选按钮，然后选择解绑定按钮，一次删除该端口下绑定的所有表项。图 5-16 显示该端口已经绑定的 mac 地址，也可绑定新的 mac 地址

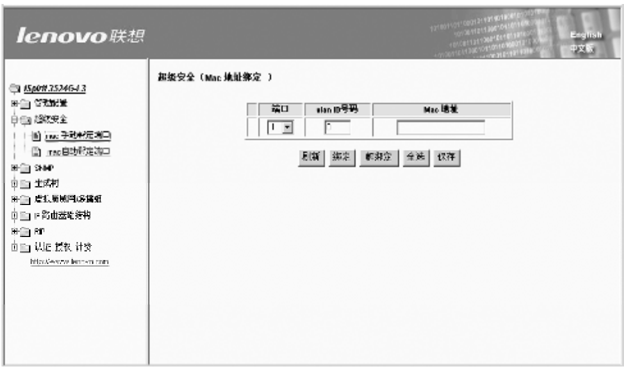


图5-16 Mac地址手动绑定页面

5.2.4.2 自动绑定

自动绑定下，当该端口没有绑定 mac 地址时，显示该端口在 avl 表中的项，亦即是学习到的 mac 地址项，此时，可以通过表中每一行前方的小方框，选择用户想要绑定的 mac 地址，可以一次选择多项，也可通过全选按钮，选择所有的项，当用户按下绑定按钮后，将会把所选 mac 地址绑定到该端口下，此时显示该端口有绑定 mac 地址的情况；当该端口下绑定有 mac 地址时，只是显示绑定在该端口下 mac 地址，并且前方不再出现小对话框。



图5-17 Mac地址自动绑定页面

5.2.5 SNMP 页面

5.2.5.1 SNMP Trap目标页面

图5-18显示SNMP Trap目标页面，该页面允许用户查看并修改一些SNMP-TARGET-MIB 对象。该页显示对象地址表及对象地址参数表。



图5-18 SNMP Trap目标页面

SNMP对象地址表上的下拉菜单中各项显示信息如下表所示。

表 5-5：

域	下拉菜单值	注释
Entry	1,2,..,行数	
Name	条目名称不可修改	
IP Address	目标IP地址	
Port	目标端口，（缺省为162）	
Timeout	重发超时的间隔时间，Snmp V1格式不支持	
Retry out	重发次数,Snmp V1格式不支持	
Snmp Version	Snmp发送trap的处理方式	
Statu S	条目的状态	

SNMP对象地址参数表上的下拉菜单中各项显示信息如表5-6所示。

表 5-6：

域	下拉菜单值	注释
Entry	条目	
Name	共用体名称如public	
View Name	访问视图，只能配置internet	
Permission	共用体的访问权限	
Status	条目的状态	

5.2.5.2 SNMP共用体名称

图 5-19 显示 Snmp 共用体名称，配置可以访问交换的共用体名称和读写权限。

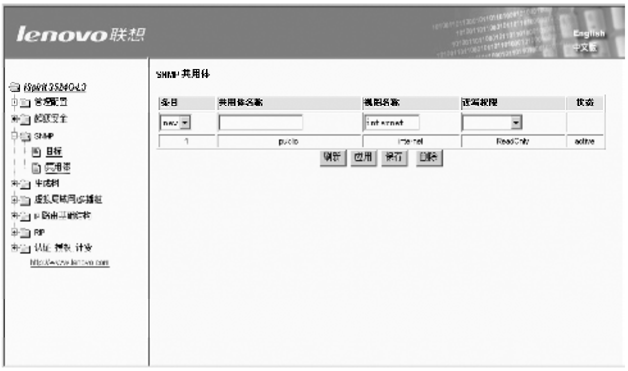


图5-19 SNMP通告页面

5.2.6 生成树页面

5.2.6.1 生成树桥(Bridge)参数设置页面

图 5-20 显示生成树桥(Bridge)参数设置页面，该页面允许用户查看并编辑生成树桥(Bridge)参数。



图5-20 生成树桥(Bridge)参数设置页面

5.2.6.2 生成树端口参数设置页面

图5-21显示生成树端口参数设置页面，该页面允许用户查看并编辑生成树端口参数。用户可以通过设置Enable域启用或禁用该端口的生成树。如果用户在这里设置启用，则需要启用相应的交换机配置页面的生成树。用户使用下拉菜单选择想要编辑的单元和端口。



图5-21生成树端口参数设置页面

页面上的下拉菜单中各项显示信息如下表所示。

表 5-10：

域	下拉菜单值	注释
Unit	1	
Port	1,2,..,26	缺省：1
Enable	enable,disable	缺省：enable

5.2.7 VLAN/ 多播组配置页面

5.2.7.1 当前 VLAN配置页面

图 5-22 显示当前 VLAN 配置页面。该页面是只读页，显示当前激活的 VLAN 配置。包含动态（GVRP）和静态（管理）VLAN 条目。当所有条目在一页显示不下时，按下 NEXT 按钮显示下一页条目。

在每一个端口处点击鼠标，可以在下表列出的端口不同值间进行切换。

表 5-11：

字符	全称	含义
-	Non-member	该端口不是这一VLAN的成员
M	Member	该端口是这一VLAN的成员
U	Untagged	为这一VLAN传递的输出包无标记

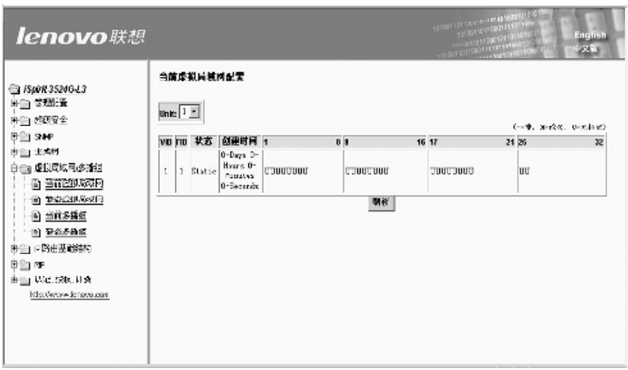


图5-22 显示当前VLAN配置页面

页面上的下拉菜单中各项显示信息如下表所示。

表 5-12：

域	下拉菜单值	注释
Unit	1	

5.2.7.2 静态 VLAN配置页面

图5-23显示静态VLAN配置页面，该读写页面允许用户一次为一个VID编辑静态VLAN配置。该页面由两部分构成：活动行和列表框。活动行在首行，可编辑。活动行下方的列表框包含一系列的以 VID 和名字标识的静态 VLAN。

为加入一个新的 VLAN，用户在活动行输入数据，然后按下应用（Apply）或存储(SAVE)键，这时列表框会显示用户创建行的 VID 和名字。

为编辑一个已经存在的 VLAN，用户需要点击列表框中相应的 VLAN。该 VLAN 将显示在活动行中，用户可以根据需要进行编辑。当编辑结束时，按下应用（APPLY)或存储（Save）键。

为删除一个 VLAN，用户需要点击列表框中相应的 VLAN。该 VLAN 将显示在活动行中，按下删除（Delete）键可以删除该 VLAN，同时该 VLAN 的信息将从列表框中删除。

在每一个端口处点击鼠标，可以在下表列出的端口不同值间进行切换。

表 5-13：

字符	全称	含义
-	Non-member	该端口不是这一VLAN的成员
M	Member	该端口是这一VLAN的tagged成员
F	Forbidden	禁止该端口成为这一VLAN的成员
U	Untagged	该端口是这一VLAN的Untaged成员



图5-23 静态VLAN配置页面

页面上的下拉菜单中各项显示信息如下表所示。

表 5-14：

域	下拉菜单值	注释
Unit	x(x=0,1,2,3……)	
VID	有效值	
Egress Ports	-，M，F，U	为每一端口选择相应值

5.2.7.3 当前多播配置页面

图5-24显示当前多播配置页面，该页面是只读页，显示当前激活的动态GMRP注册和静态多播组配置。VLAN ID和MAC地址是目录。当所有条目在一页显示不下时，按下NEXT按钮显示下一页条目。



图5-24当前多播配置页面

页面上的下拉菜单中各项显示信息如表5-16所示。

表5-16：

域	下拉菜单值	注释
Unit	1	

5.2.7.4 静态多播配置页面

图5-25显示静态多播配置页面，该读写页面允许用户一次为一个VID和一个MAC地址编辑静态多播组。该页面由两部分构成：活动行和列表框。活动行在首行，可编辑。活动行下方的列表框包含一系列的以VID和MAC地址标识的静态多播组。

为加入一个新的多播组，用户在活动行中输入数据，然后按下应用（APPLY）或存储（Save）键，这时列表框会显示用户创建行的VID和MAC地址。



图5-25静态多播配置页面

为编辑一个已经存在的多播组，用户需要点击列表框中相应的多播组。该多播组将显示在活动行中，用户可以根据需要进行编辑。当编辑结束时，按下应用（APPLY)或存储（Save）键。

为删除一个多播组，用户需要点击列表框中相应的多播组。该多播组将显示在活动行中，按下 Delete 键可以删除该多播组，同时该多播组的信息将从列表框中删除。

在每一个端口处点击鼠标，可以在下表列出的端口不同值间进行切换。

表 5-17：

字符	全称	含义
-	Non-member	该端口不是这一GMRP的成员
M	Member	该端口是这一GMRP的成员
F	Forbidden	禁止该端口成为这一GMRP的成员

页面上的下拉菜单中各项显示信息如下表所示。

表 5-18：

域	下拉菜单值	注释
Unit	1	
VID	Valid values	
MAC Address	Valid values	
Egress Ports	-，M，F	为每一端口选择相应值

5.2.8 IP 子网配置页面

图5-26显示当前交换机对于与vlan相关联子网配置情况。在该页面可以添加子网，或修改与vlan、接口相关的子网参数。一个vlan可以配置多个子网，一个接口仅可以配置一个子网。当状态显示active时表示该IP子网可用。

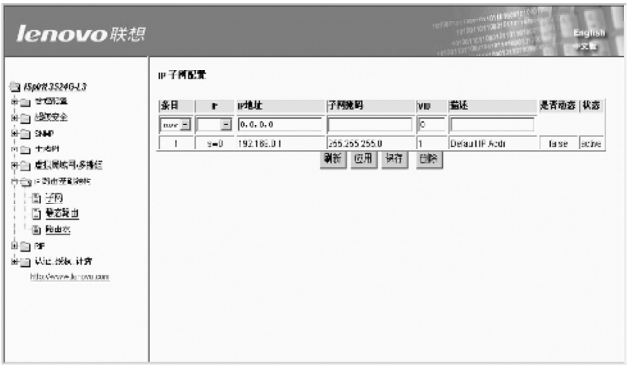


图5-26 IP子网配置页面

5.2.9 静态路由配置页面

图5-27显示当前交换机静态路由配置情况。在该页面可以添加或修改一条静态路由。这里的目的地址为一个网络IP地址，即目的地址和子网掩码的与运算等于目的地址。下一条地址为ip地址，该地址必须与现有的交换机子网络地址在同一个网段。



图5-27 静态路由配置页面

5.2.10 IP 路由表页面

显示当前交换机的路由表信息,包括静态路由信息和动态路由协议学习到的路由信息。



图5-28 IP路由表页面

5.2.11 RIP 配置页面

图5-29显示现存接口对RIP协议的配置情况。在该页面可以修改指定接口的RIP协议各个字段的配置信息。该网页只有在RIP协议启动后才能显示。

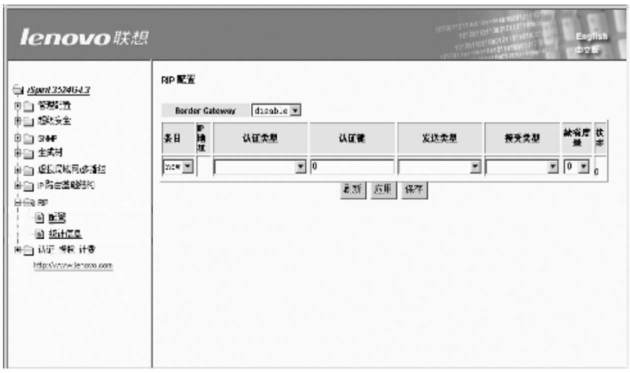


图5-29 RIP配置页面

5.2.12 RIP 统计信息页面

图5-30显示交换机运行RIP协议后的一些统计信息，从IP地址上可以具体看到各个接口的情况。该网页只有在RIP协议启动后才能显示。



图5-30 RIP统计信息页面

5.2.13 认证.授权.计费

5.2.13.1 Radius 配置

如图5-31显示认证服务器在交换机上的配置页面。可设置的信息包括：

1.radius 服务器 ip 地址，若服务器为本交换机，设为 local；
2.备用服务器 ip 地址；
3.认证 UDP 端口，默认值的服务器端口号为 1812，一般不用改；
4.是否启动计费；
5.计费 UDP 端口号，一般为 1813，不用改；
6.共享密钥，用来设定交换机与服务器之间的加密密码；
7.厂商特定信息；
8.NAS 端口、NAS 端口类型、NAS 服务类型，这三个值不用做修改。

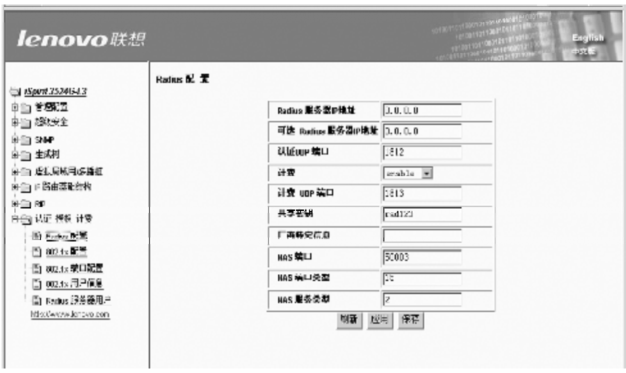


图5-31 Radius 配置页面

5.2.13.2 802.1x协议参数配置

图 5-32 显示交换机上的 802.1x 协议配置情况。包括：

1.是否启动 1x 协议；
2.是否打开重新认证功能；
3.设置重新认证时间间隔；
4.Quiet Period 定时器；
5.Tx-Period 定时器；
6.Server timeout 定时器；
7.supplicant timeout 定时器；
8.Max Request个数，包括用户端向交换机和交换机向用户重新提交失败包的最多个数；
9.认证过程失败，重新认证的最多次数。

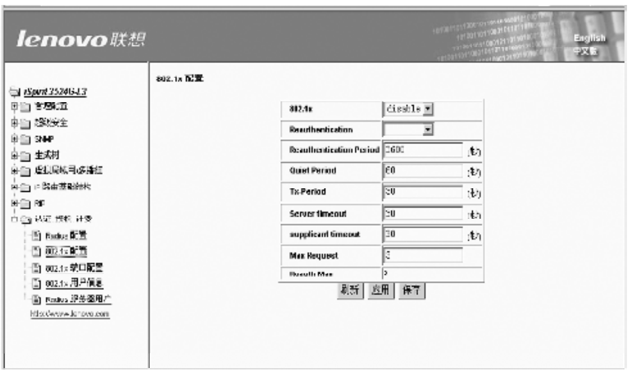


图5-32 802.1x协议参数配置页面

5.2.13.3 802.1x协议对端口的配置

图5-33显示管理员对交换机各个端口关于802.1x的配置情况。每一个端口可以配置为：支持强制认证、强制非认证、认证和不支持认证四种状态。还可以设置每个端口支持的最多用户个数。

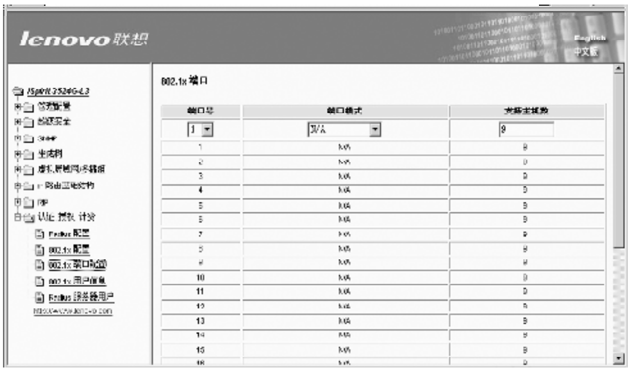


图5-33 802.1x协议对端口的配置页面

5.2.13.4 用户在交换机上的认证状态

图5-34显示交换机上用户的认证状态。可以看见在某端口上用户的认证状态，包括：用户名、mac 地址、认证状态等信息。



图5-34 802.1x配置页面

5.2.13.5 用户信息管理

图5-35显示了用户的信息维护页面。在该页面下可以看见交换机作为认证服务器时设置的用户信息，用户信息包括：用户名、密码、截止日期。管理员可以通过点击添加按钮添加一个用户。点击修改按钮修改某用户的信息。



图5-35 802.1x Radius服务器用户配置页面

第6章
常见问题解答

用户可以从控制台和Web网页上获取相应的统计信息来诊断问题,具体内容参考第4章、第5 章。

常见交换机问题分为以下几类：

- ➲ 低性能
- ➲ 无连接

下面详细说明如何判断并解决这些问题,如果需要更多的技术咨询和支持,请联系本公司的技术支 持。

现象 1 性能下降、错误过多。

可能的起因	解决办法
➲双工自协商出现不匹配	考查通信双方的自协商设置，识别是否出现自协商不匹配的情况
➲网线长度超过规定长度	
❶ 端口统计信息显示很多冲突（late-collision）和排队错误。	参考第三章获取显示端口统计的帧检查序列、碰撞信息的相关内容 。

可能的起因	解决办法
❷ 对于10/100BaseTX连接端口与所连设备的距离超过 140 米。	将网线的长度减小到规定的长度范围内 。
❸ 对于1000BaseTX连接端口与所连设备的距离超过 100 米。	将网线的长度减小到规定的长度范围内 。

➲所连设备的网卡损坏

❶ 端口统计信息出现很多错误。	运行网卡诊断程序。

现象 2 *无连接*

可能的起因	解决办法

➲ 使用了不正确或损坏了的网线。

以下现象表明双方无连接：

网线跳线错误。	以一根测试过的网线替换原来的网线 。

附录 A
产品特征参数

接口	
	24个10Base-T/100/1000Base-TX RJ-45 UTP-5端口 1个GBIC接口扩展插槽 2个10/100/1000Base-T RJ-45 UTP-5端口 1个UART控制端口
物理特点	
	重量：5KG 尺寸：444mm × 44.45mm × 348mm(W × H × L)
环境要求	
温度	操作： 0ºC to 40ºC (32ºF to 104ºF) 存储： -20ºC to 70ºC (-4ºF to 158ºF)
湿度	操作： 10% to 90% RH 存储： 5% to 90% RH
海拔	操作:最高3000米(10,000英尺) 存储:最高4570米(15,000英尺)

表A-1 联想天工iSpirit 3524G-L3/iSpirit 3524F-L3交换机产品技术指标

网络媒体	
10Base-T:	UTP Category 3, Category 4或Category 5网线
100Base-TX:	UTP Category 5网线
1000Base-X:	1000Base-SX,1000Base-LX/LH或1000Base-ZX光纤
10/100/1000Base-T:	UTP Category 5网线或UTP Category 5 Enhanced网线
控制端口：	**专用串口线**
电源要求	
电压范围	180-264V**交流电源输入**
电流限制	**最大** 1.5A

表A-1**续 联想天工**iSpirit 3524G-L3/iSpirit 3524F-L3**交换机产品技术指标**

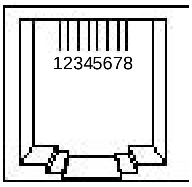
附录B
接口与网线的技术说明

附录B**说明联想天工**iSpirit 3524G-L3/iSpirit 3524F-L3**交换机网口和网线的技术特征。**

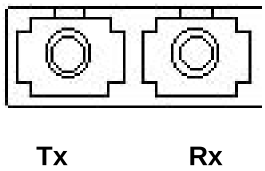
接口说明

10/100Base-T端口

10/100Base-T **以太网端口使用标准** RJ-45 **接头。端口的发送信号**（TD）**和接收信号**（RD）**内部交叉。由交换机实现直连网线与交叉网线的自协商，所以与这些端口连接时可以使用直连网线或交叉网线。图** B-1 **显示** 10/100Base-T **端口的管脚排列。**



图B-1 10/100Base-T端口的管脚



图B-2 1000 Base-X双SC接口

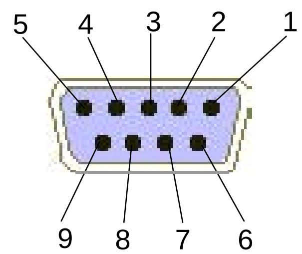
1000 Base-X **端口使用标准的双** SC **接口，如图** B-2 **所示。**

10/100/1000Base-T端口

10/100/1000 Base-T端口使用标准RJ-45接口和内部交叉的引脚排列方式。这些端口的发送信号（TD）和接收信号（RD）内部交叉。内部硬件实现直连网线与交叉网线的自协商，所以与这些端口连接时可以使用直连网线或交叉网线。10/100/1000Base-T端口的管脚如图B-1所示。

控制端口

交换机控制端口使用标准的9针UART接口。UART接口的管脚如图B-3所示。



图B-3 UART接口的管脚

控制端口专用电缆的管脚说明如表B-3所示。

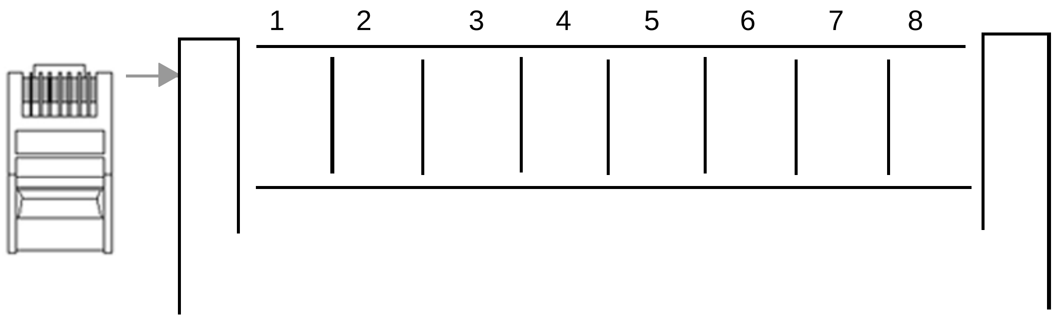
表B-3 控制端口专用电缆的管脚说明:

电缆一端信号	DB-9管脚	DB-9管脚	电缆另一端信号
DCD	1	1	DCD
RXD	2	3	TXD
TXD	3	2	RXD
DTR	4	4	DTR
SIG GND	5	5	SIG GND
DSR	6	6	DSR
RTS	7	7	RTS
CTS	8	8	CTS
RI	9	9	RI

网线说明

交叉和直连双绞线管脚说明

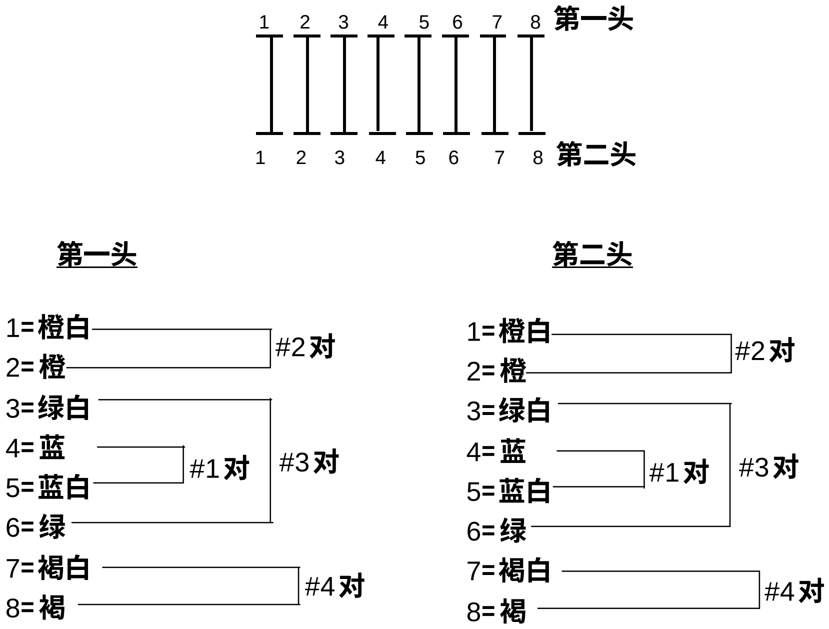
1.**直连和交叉双绞线管脚示意图如** B-4 **所示。**



图B-4 RJ-45双绞线管脚示意图

2.**直连双绞线的国际标准**

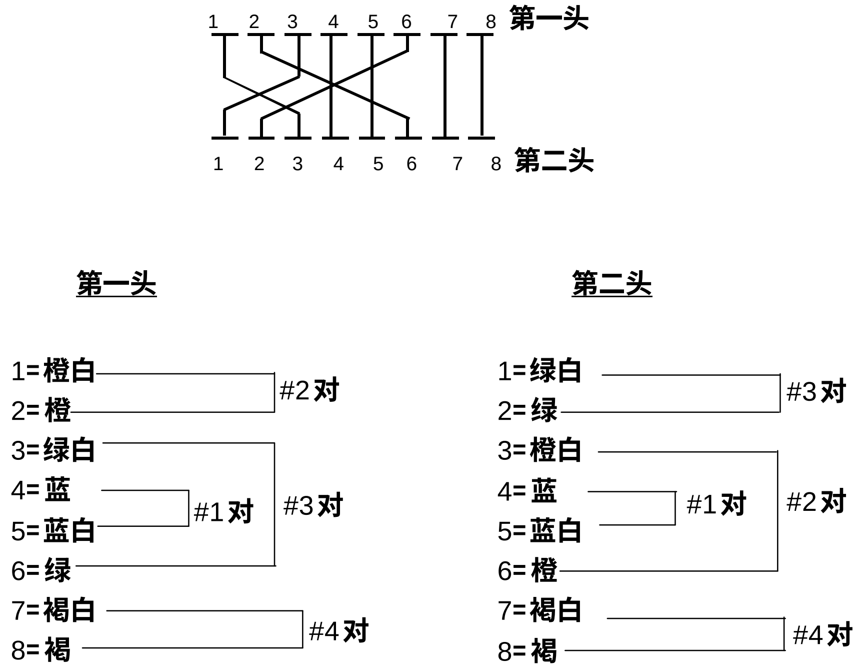
直接连结双绞线的接线方法的国际标准如图 B-5 **所示，其主要特点是，双绞线两头** SIDE1、SIDE2 **两方的接线顺序一样，并且接到** RJ-45 **头** 3、6 **针上的是同一对双绞线。**



图B-5 RJ-45直连双绞线的国际标准

3.交叉对连双绞线的国际标准

交叉对连双绞线的接线方法的国际标准如图 B-6 所示，其主要特点是，双绞线两头 SIDE1、SIDE2 两方的接线顺序不一样，其连接如下图所示。



图B-6 RJ-45交叉对连双绞线的国际标准